PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-320478
(43)Date of publication of application : 04.12.1998

(51)Int.Cl. G06F 17/60
G09C 1/00

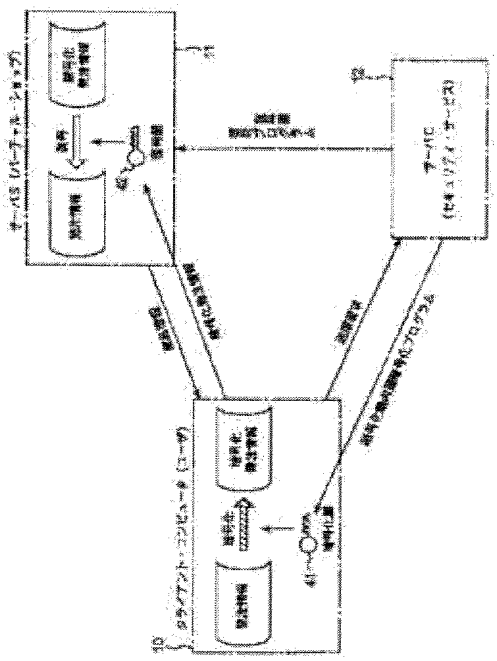
(21)Application number : 10-089577
(22)Date of filing : 19.03.1998

(71)Applicant : PUMPKIN HOUSE:KK
(72)Inventor : SASAKI MINORU

(30)Priority
Priority number : 09 85955 Priority date : 19.03.1997 Priority country : JP

(54) CIPHERED/DECIPHERED COMMUNICATION SYSTEM AND METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide transmit data security without burdening a user by making a ciphering process and a deciphering process for data which are transmitted and received through a communication line correspond to each other.
SOLUTION: A deciphering key 42 and a deciphering program are delivered from a server C12 to a server S11 in advance. A client computer 10 receives article information from the server S11 through a network. When order information is inputted and an order button is clicked, the deciphering program having a ciphering key 41 inside is sent from the server C12 to the client computer 10. The client computer 10 ciphers the order information according to the deciphering program by using the ciphering key 41 and sends the information to the server S11. The server S11 deciphers the received ciphered order information according to the deciphering program to obtain the original order information.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－320478

(43)公開日　平成10年(1998)12月４日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｂ

審査請求　未請求　請求項の数56　ＦＤ　（全 36 頁）

(21)出願番号　特願平10－89577

(22)出願日　平成10年(1998)３月19日

(31)優先権主張番号　特願平9－85955

(32)優先日　平９(1997)３月19日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　393009356
株式会社パンプキンハウス
神奈川県厚木市飯山1620番地の１　アメニテイヒル本厚木717

(72)発明者　佐々木　實
神奈川県厚木市飯山1620番地の１　アメニティヒル本厚木717　株式会社パンプキンハウス内

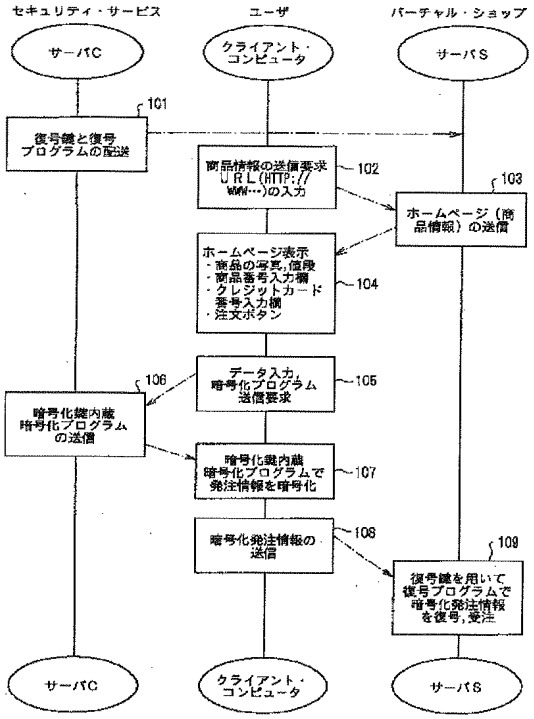
(74)代理人　弁理士　牛久　健司

(54)【発明の名称】　暗号化／復号通信システムおよび方法

(57)【要約】

【目的】　通信回線を通じて送受信されるデータの暗号化処理と，復号処理とを対応させ，ユーザに負担をかけることなく，送信データの機密化を図る。

【構成】　復号鍵42と復号プログラムとが，サーバＣ12からサーバＳ11にあらかじめ配送される。クライアント・コンピュータ10は，サーバＳ11から商品情報をネットワーク13を通じて受信する。発注情報を入力し注文ボタンをクリックすると，クライアント・コンピュータ10にはサーバＣ12から暗号化鍵41を内蔵した暗号化プログラムが送信される。クライアント・コンピュータ10は発注情報を暗号化鍵41を用いて暗号化プログラムにしたがって暗号化し，サーバＳ11に送信する。サーバＳ11は受信した暗号化発注情報を，復号鍵42を用いて復号プログラムにしたがって復号し，もとの発注情報を得る。



1

【特許請求の範囲】

【請求項１】　クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法において，上記セキュリティサービス・サーバに，少なくとも第１の暗号化鍵，および上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラムを保持させておき，上記バーチャルショップ・サーバに，第１の復号鍵および上記第１の暗号化プログラムによって暗号化されたデータを第１の復号鍵を用いて復号するための第１の復号プログラムを保持させておき，上記バーチャルショップ・サーバに商品情報を保持させておき，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記バーチャルショップ・サーバから上記クライアント・コンピュータに上記商品情報を送信し，上記クライアント・コンピュータから上記セキュリティサービス・サーバに第２の送信要求を送信し，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記第１の暗号化鍵および上記第１の暗号化プログラムを送信し，上記クライアント・コンピュータは，送信された上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信し，上記バーチャルショップ・サーバは，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記商品発注情報を復号する，暗号化通信による商品注文方法。

【請求項２】　上記第１の暗号化鍵と上記第１の復号鍵が，データの暗号化と復号に共通に用いられる秘密鍵である，請求項１に記載の暗号化通信による商品注文方法。

【請求項３】　上記第１の暗号化プログラムおよび上記第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記第１の暗号化鍵が公開鍵，上記第１の復号鍵が秘密鍵である，請求項１に記載の暗号化通信による商品注文方法。

【請求項４】　上記セキュリティサービス・サーバに消去プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記消去プログラムを送信し，上記クライアント・コンピュータは，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信した後，上記消去プログラムにしたがって上記第１の暗号化プログラムおよび上記第１の暗号化鍵のうち少なくともいずれか一つを消去する，請求項１から３のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項５】　クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法において，上記セキュリティサービス・サーバに，少なくとも第１の暗号化鍵，第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持させておき，上記バーチャルショップ・サーバに，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，および上記第２の暗号化プログラムによって暗号化されたデータを上記第２の暗号化／復号鍵を用いて復号するための第２の復号プログラムを保持させておき，上記バーチャルショップ・サーバに商品情報を保持させておき，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記バーチャルショップ・サーバから上記クライアント・コンピュータに上記商品情報を送信し，上記クライアント・コンピュータから上記セキュリティサービス・サーバに第２の送信要求を送信し，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記第１の暗号化鍵，上記第１の暗号化プログラムおよび上記第２の暗号化プログラムを送信し，上記クライアント・コンピュータは，上記第２の暗号化／復号鍵を用いて，送信された上記第２の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，暗号化された上記商品発注情報と，暗号化された上記第２の暗号化／復号鍵とを上記バーチャルショップ・サーバに送信し，上記バーチャルショップ・サーバは，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号化された上記商品発注情報を復号する，暗号化通信による商品注文方法。

【請求項６】　上記第１の暗号化鍵と上記第１の復号鍵がデータの暗号化と復号とに共通に用いられる秘密鍵である，請求項５に記載の暗号化通信による商品注文方法。

【請求項７】　上記第１の暗号化プログラムおよび第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記第１の暗号化鍵が公開鍵，上記第１の復号鍵が秘密鍵である，請求項５に記載の暗号化通信による商品注文方法。

【請求項８】　上記第１の暗号化プログラムと上記第２の暗号化プログラムとが同じものであり，上記第１の復号プログラムと上記第２の復号プログラムとが同じものである，請求項５に記載の暗号化通信による商品注文方

法。

【請求項９】　上記第２の暗号化／復号鍵が，上記クライアント・コンピュータに入力される入力値である，請求項５に記載の暗号化通信による商品注文方法。

【請求項１０】　上記セキュリティサービス・サーバに，乱数生成プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記乱数生成プログラムを送信し，上記クライアント・コンピュータは上記乱数生成プログラムによって乱数を生成し，この生成した乱数を上記第２の暗号化／復号鍵として用いる，請求項５に記載の暗号化通信による商品注文方法。

【請求項１１】　上記セキュリティサービス・サーバに消去プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記消去プログラムを送信し，上記クライアント・コンピュータは，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信した後，上記消去プログラムにしたがって上記第１および第２の暗号化プログラム，上記第１の暗号化鍵，上記第２の暗号化／復号鍵，ならびに乱数生成プログラムのうち少なくともいずれか一つを消去する，請求項10に記載の暗号化通信による商品注文方法。

【請求項１２】　上記バーチャルショップ・サーバが複数台あり，上記第１の暗号化鍵と上記第１の復号鍵との対が上記バーチャルショップ・サーバごとにそれぞれ異なるものであり，上記セキュリティサービス・サーバに，すべての上記第１の暗号化鍵を保持させておき，上記バーチャルショップ・サーバに，それぞれに固有の第１の復号鍵を保持させておき，上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，商品を発注すべき上記バーチャルショップ・サーバを識別するためのショップ識別子を送信し，上記セキュリティサービス・サーバは，送信されたショップ識別子に対応する第１の暗号化鍵を選んで上記クライアント・コンピュータに送信する，請求項１から11のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１３】　上記第１の暗号化鍵と上記第１の復号鍵との対が複数のユーザごとにそれぞれ異なるものであり，上記セキュリティサービス・サーバに，すべてのユーザの第１の暗号化鍵を保持させておき，上記バーチャルショップ・サーバに，そのバーチャルショップ・サーバにアクセスが許されたすべてのユーザの第１の復号鍵を保持させておき，上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，発注を行うユーザを識別するためのユーザ識別子を送信し，上記セキュリティサービス・サーバは，送信されたユーザ識別子に対応する第１の暗号化鍵を選んで上記クライアント・コンピュータに送信し，暗号化された上記商品発注情報とともに，上記クライアント・コンピュータから上記バーチャルショップ・サーバに発注を行うユーザのユーザ識別子を送信し，上記バーチャルショップ・サーバは，送信されたユーザ識別子に対応する第１の復号鍵を選んで，暗号化された上記商品発注情報を復号する，請求項１から12のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１４】　上記バーチャルショップ・サーバから上記クライアント・コンピュータに送信される上記商品情報に，上記セキュリティサービス・サーバのアドレスを含ませておき，上記クライアント・コンピュータは上記アドレスに上記第２の送信要求を送信する，請求項１から13のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１５】　上記クライアント・コンピュータは上記セキュリティショップ・サーバから送信される暗号化プログラムを含むプログラムを受信すると，このプログラムにしたがって，ユーザの介入なしに，商品発注情報の暗号化と暗号化された商品発注情報のバーチャルショップ・サーバへの送信とを自動的に行う，請求項１から14のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１６】　上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信される上記第１の暗号化鍵が，上記第１の暗号化プログラムに内蔵されているものである，請求項１から15のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１７】　上記バーチャルショップ・サーバとセキュリティサービス・サーバとが別個のコンピュータ・システムであり，通信手段により相互に接続可能である，または，上記バーチャルショップ・サーバとセキュリティサービス・サーバとが同一のコンピュータ・システムである，請求項１から16のいずれか一項に記載の暗号化通信による商品注文方法。

【請求項１８】　第１の装置が第２の装置および第３の装置と通信手段を介して接続可能な暗号化／復号通信方法において，上記第２の装置に，暗号化鍵と，この暗号化鍵を用いてデータを暗号化するための暗号化プログラムとを保持させておき，上記第１の装置からの送信要求に応答して，上記第２の装置から上記第１の装置に上記暗号化鍵および上記暗号化プログラムを送信し，上記第１の装置は，送信された上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第３の装置に送信する，暗号化／復号通信方法。

【請求項１９】　上記第３の装置に，復号鍵と，上記暗号化プログラムによって暗号化されたデータを上記復号鍵を用いて復号するための復号プログラムとを保持させておき，上記第３の装置は，上記復号鍵を用いて上記復号プログラムにしたがって，上記第１の装置から送信さ

れた暗号文データを復号する，請求項18に記載の暗号化／復号通信方法。

【請求項２０】　上記第３の装置は，上記第１の装置からの要請に応じて，上記第２の装置のアドレスを含むデータを上記第１の装置に送信し，上記第１の装置は上記アドレスに上記送信要求を送信する，請求項18に記載の暗号化／復号通信方法。

【請求項２１】　上記暗号化鍵と上記復号鍵がデータの暗号化と復号に共通に用いられる秘密鍵である，請求項19に記載の暗号化／復号通信方法。

【請求項２２】　上記暗号化プログラムおよび上記復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記暗号化鍵が公開鍵，上記復号鍵が秘密鍵である，請求項19に記載の暗号化／復号通信方法。

【請求項２３】　上記第２の装置に消去プログラムを保持させておき，上記送信要求に応答して，上記第２の装置から上記第１の装置に上記消去プログラムを送信し，上記第１の装置は，上記暗号文データを上記第３の装置に送信した後，上記消去プログラムにしたがって上記暗号化プログラムおよび上記暗号化鍵のうち少なくともいずれか一つを消去する，請求項18から22のいずれか一項に記載の暗号化／復号通信方法。

【請求項２４】　第１の装置が第２の装置および第３の装置と通信手段を介して接続可能な暗号化／通信方法において，上記第２の装置に，第１の暗号化鍵，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持させておき，上記第１の装置からの送信要求に応答して，上記第２の装置から上記第１の装置に上記第１の暗号化鍵，上記第１の暗号化プログラムおよび上記第２の暗号化プログラムとを送信し，上記第１の装置は，上記第２の暗号化／復号鍵を用いて，送信された上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第３の装置に送信する，暗号化／復号通信方法。

【請求項２５】　上記第３の装置に，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，および上記第２の暗号化プログラムによって暗号化されたデータを上記第２の暗号化／復号鍵を用いて復号するための第２の復号プログラムを保持させておき，上記第３の装置は，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号文データを復号する，請求項24に記載の暗号化／復号通信方法。

【請求項２６】　上記第３の装置は，上記第１の装置からの要請に応じて，上記第２の装置のアドレスを含むデータを上記第１の装置に送信し，上記第１の装置は上記アドレスに上記送信要求を送信する，請求項24に記載の暗号化／復号通信方法。

【請求項２７】　上記第１の暗号化鍵と上記第１の復号鍵がデータの暗号化と復号とに共通に用いられる秘密鍵である，請求項25に記載の暗号化／復号通信方法。

【請求項２８】　上記第１の暗号化プログラムおよび第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記第１の暗号化鍵が公開鍵，上記第１の復号鍵が秘密鍵である，請求項25に記載の暗号化／復号通信方法。

【請求項２９】　上記第１の暗号化プログラムと上記第２の暗号化プログラムとが同じものであり，上記第１の復号プログラムと上記第２の復号プログラムとが同じものである，請求項25に記載の暗号化／復号通信方法。

【請求項３０】　上記第２の暗号化／復号鍵が，上記第１の装置に入力される入力値である，請求項25に記載の暗号化／復号通信方法。

【請求項３１】　上記第２の装置に，乱数生成プログラムを保持させておき，上記第２の送信要求に応答して，上記第２の装置から上記第１の装置に上記乱数生成プログラムを送信し，上記第１の装置は上記乱数生成プログラムによって乱数を生成し，この生成した乱数を上記第２の暗号化／復号鍵として用いる，請求項25に記載の暗号化／復号通信方法。

【請求項３２】　上記第２の装置に消去プログラムを保持させておき，上記第２の送信要求に応答して，上記第２の装置から上記第１の装置に上記消去プログラムを送信し，上記第１の装置は，暗号化された上記商品発注情報を上記第３の装置に送信した後，上記消去プログラムにしたがって上記第１および第２の暗号化プログラム，上記第１の暗号化鍵，上記第２の暗号化／復号鍵，ならびに乱数生成プログラムのうち少なくともいずれか一つを消去する，請求項31に記載の暗号化／復号通信方法。

【請求項３３】　上記第２の装置と上記第３の装置とが別個のコンピュータ・システムであり，通信手段により相互に接続可能である，または，上記第２の装置と上記第３の装置とが同一のコンピュータ・システムである，請求項18から32のいずれか一項に記載の暗号化／復号通信方法。

【請求項３４】　上記第１の装置は上記第２の装置から送信される暗号化プログラムを含むプログラムを受信すると，このプログラムにしたがって，ユーザの介入なしは，データの暗号化と暗号化データの第３の装置への送信とを自動的に行う，請求項18から33のいずれか一項に記載の暗号化／復号通信方法。

【請求項３５】　第１の装置，第２の装置および第３の装置を含み，上記第１の装置が上記第２の装置および上記第３の装置と通信手段を介して接続可能な暗号化／復号通信システムにおいて，上記第２の装置は，暗号化鍵と，この暗号化鍵を用いてデータを暗号化するための暗号化プログラムとを保持しており，上記第１の装置からの送信要求に応答して，上記第１の装置に上記暗号化鍵と上記暗号化プログラムとを送信するものであり，上記第１の装置は，上記第２の装置から送信された上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第３の装置に送信するものである，暗号化／復号通信システム。

【請求項３６】　上記第３の装置は，復号鍵と，上記暗号化プログラムによって暗号化されたデータを上記復号鍵を用いて復号するための復号プログラムとを保持しており，上記復号鍵を用いて上記復号プログラムにしたがって，上記第１の装置から送信された暗号文データを復号するものである，請求項35に記載の暗号化／復号通信システム。

【請求項３７】　上記第３の装置は，上記第１の装置からの要請に応じて，上記第２の装置のアドレスを含むデータを上記第１の装置に送信するものであり，上記第１の装置は上記アドレスに上記送信要求を送信するものである，請求項35に記載の暗号化／復号通信システム。

【請求項３８】　第１の装置，第２の装置および第３の装置を含み，上記第１の装置が上記第２の装置および上記第３の装置と通信手段を介して接続可能な暗号化／通信システムにおいて，上記第２の装置は，第１の暗号化鍵，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持しており，上記第１の装置からの送信要求に応答して，上記第１の装置に上記第１の暗号化鍵と上記第１の暗号化プログラムと上記第２の暗号化プログラムとを送信するものであり，上記第１の装置は，上記第２の暗号化／復号鍵を用いて，上記第２の装置から送信された上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記第１の暗号化鍵を用いて，上記第１の暗号化プログラムにしたがって，上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第３の装置に送信するものである，暗号化／復号通信システム。

【請求項３９】　上記第３の装置は，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，および上記第２の暗号化プログラムによって暗号化されたデータを上記第２の暗号化／復号鍵を用いて復号するための第２の復号プログラムを保持しており，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号文データを復号するものである，請求項38に記載の暗号化／復号通信システム。

【請求項４０】　上記第３の装置は，上記第１の装置からの要請に応じて，上記第２の装置のアドレスを含むデータを上記第１の装置に送信するものであり，上記第１の装置は上記アドレスに上記送信要求を送信するものである，請求項38に記載の暗号化／復号通信システム。

【請求項４１】　クライアント・コンピュータと，バーチャルショップ・サーバと，セキュリティサービス・サーバとから構成され，上記クライアント・コンピュータは上記バーチャルショップ・サーバおよび上記セキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，上記クライアント・コンピュータから上記バーチャルショップ・サーバに商品を注文するシステムにおいて，上記バーチャルショップ・サーバは，第１の復号鍵および上記第１の暗号化プログラムによって暗号化されたデータを第１の復号鍵を用いて復号するための第１の復号プログラム，ならびに商品情報を保持しており，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記クライアント・コンピュータに上記商品情報を送信するものであり，上記クライアント・コンピュータは，上記セキュリティサービス・サーバに第２の送信要求を送信するものであり，上記セキュリティサービス・サーバは，少なくとも第１の暗号化鍵，および上記第１の鍵を用いてデータを暗号化するための第１の暗号化プログラムを保持しており，上記クライアント・コンピュータからの上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記第１の暗号化鍵および上記第１の暗号化プログラムを送信するものであり，上記クライアント・コンピュータはさらに，上記第１の暗号化鍵を用いて，上記セキュリティサービス・サーバから送信された上記第１の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信するものであり，上記バーチャルショップ・サーバはさらに，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記商品発注情報を復号するものである，暗号化通信による商品注文システム。

【請求項４２】　クライアント・コンピュータと，バーチャルショップ・サーバと，セキュリティサービス・サーバとから構成され，上記クライアント・コンピュータは上記バーチャルショップ・サーバおよび上記セキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，上記クライアント・コンピュ

ータから上記バーチャルショップ・サーバに商品を注文するシステムにおいて，上記バーチャルショップ・サーバは，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，および上記第２の暗号化プログラムによって暗号化されたデータを第２の暗号化／復号鍵を用いて復号するための第２の復号プログラム，ならびに商品情報を保持しており，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記クライアント・コンピュータに上記商品情報を送信ものであり，上記クライアント・コンピュータは，上記セキュリティサービス・サーバに第２の送信要求を送信するものであり，上記セキュリティサービス・サーバは，少なくとも第１の暗号化鍵，第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持しており，上記クライアント・コンピュータからの上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記第１の暗号化鍵，上記第１の暗号化プログラムおよび上記第２の暗号化プログラムとを送信するものであり，上記クライアント・コンピュータはさらに，上記第２の暗号化／復号鍵を用いて，上記セキュリティサービス・サーバから送信された上記第２の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，暗号化された上記商品発注情報と，暗号化された上記第２の暗号化／復号鍵とを上記バーチャルショップ・サーバに送信するものであり，上記バーチャルショップ・サーバはさらに，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号化された上記商品発注情報を復号するものである，暗号化通信による商品注文システム。

【請求項４３】　クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法において，上記クライアント・コンピュータから上記バーチャルショップ・サーバに第１の送信要求を送信し，上記第１の送信要求に応答して上記バーチャルショップ・サーバから送信される商品情報と上記セキュリティサービス・サーバのアドレスとを上記クライアント・コンピュータが受信し，上記受信したアドレスにしたがって上記セキュリティサービス・サーバに上記クライアント・コンピュータから第２の送信要求を送信し，上記第２の送信要求に応答して上記セキュリティサービス・サーバから送信される第１の暗号化鍵と第１の暗号化プログラムとを上記クライアント・コンピュータが受信し，上記クライアント・コンピュータは，受信した上記暗号化鍵を用いて上記暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信する，クライアント・コンピュータによる商品注文方法。

【請求項４４】　バーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，バーチャルショップ・サーバに商品を注文するクライアント・コンピュータにおいて，上記バーチャルショップ・サーバに第１の送信要求を送信し，上記第１の送信要求に応答して上記バーチャルショップ・サーバから送信される商品情報と上記セキュリティサービス・サーバのアドレスとを受信し，上記受信したアドレスにしたがって上記セキュリティサービス・サーバに第２の送信要求を送信し，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから送信される第１の暗号化鍵と第１の暗号化プログラムとを受信し，受信した上記暗号化鍵を用いて上記暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信するものである，クライアント・コンピュータ。

【請求項４５】　クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法において，上記クライアント・コンピュータから上記バーチャルショップ・サーバに第１の送信要求を送信し，上記第１の送信要求に応答して上記バーチャルショップ・サーバから送信される商品情報と上記セキュリティサービス・サーバのアドレスとを上記クライアント・コンピュータが受信し，上記受信したアドレスにしたがって上記セキュリティサービス・サーバに上記クライアント・コンピュータから第２の送信要求を送信し，上記第２の送信要求に応答して上記セキュリティサービス・サーバから送信される第１の暗号化鍵と，第１の暗号化プログラムと，第２の暗号化プログラムとを上記クライアント・コンピュータが受信し，上記クライアント・コンピュータは，第２の暗号化／復号鍵を用いて，上記第２の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，上記第１の暗号化鍵を用いて上記第１の暗号プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，暗号化された上記商品発注情報と，暗号化された上記第２の暗号化／復号鍵とを上記バーチャルショップ・サーバに送信する，クライアント・コンピュータによる商品注文方法。

【請求項４６】　バーチャルショップ・サーバおよびセ

キュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，バーチャルショップ・サーバに商品を注文するクライアント・コンピュータにおいて，上記バーチャルショップ・サーバに第１の送信要求を送信し，上記第１の送信要求に応答して上記バーチャルショップ・サーバから送信される商品情報と上記セキュリティサービス・サーバのアドレスとを受信し，上記受信したアドレスにしたがって上記セキュリティサービス・サーバに第２の送信要求を送信し，上記第２の送信要求に応答して上記セキュリティサービス・サーバから送信される第１の暗号化鍵と第１の暗号化プログラムと第２の暗号化プログラムとを受信し，上記第２の暗号化／復号鍵を用いて，上記第２の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，暗号化された上記商品発注情報と，暗号化された上記第２の暗号化／復号鍵とを上記バーチャルショップ・サーバに送信するものである，クライアント・コンピュータ。

【請求項４７】　第１の装置が第２の装置および第３の装置と通信手段を介して接続可能であり，暗号化通信によって上記第１の装置から上記第３の装置にデータを送信する方法において，上記第１の装置から上記第３の装置に第１の送信要求を送信し，上記第１の送信要求に応答して上記第３の装置から送信されるデータと上記第２の装置のアドレスとを上記第１の装置が受信し，上記受信したアドレスにしたがって上記第２の装置に上記第１の装置から第２の送信要求を送信し，上記第２の送信要求に応答して上記第２の装置から送信される暗号化鍵と暗号化プログラムとを上記第１の装置が受信し，上記第１の装置は，受信した上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第３の装置に送信する，暗号化通信方法。

【請求項４８】　コンピュータ装置において，このコンピュータ装置は他の第１の装置および他の第２の装置と通信手段を介して接続可能であり，さらにこのコンピュータ装置は，上記第２の装置に第１の送信要求を送信し，上記第１の送信要求に応答して上記第２の装置から送信されるデータと上記第１の装置のアドレスとを受信し，上記受信したアドレスにしたがって上記第１の装置に第２の送信要求を送信し，上記第２の送信要求に応答して上記第１の装置から送信される暗号化鍵と暗号化プログラムとを受信し，受信した上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第２の装置に送信するものである，コンピュータ装置。

【請求項４９】　第１の装置が第２の装置および第３の装置と通信手段を介して接続可能であり，暗号化通信によって上記第１の装置から上記第３の装置にデータを送信する方法において，上記第１の装置から上記第３の装置に第１の送信要求を送信し，上記第１の送信要求に応答して上記第３の装置から送信されるデータと上記第２の装置のアドレスとを上記第１の装置が受信し，上記受信したアドレスにしたがって上記第２の装置に上記第１の装置から第２の送信要求を送信し，上記第２の送信要求に応答して上記第２の装置から送信される第１の暗号化鍵と第１の暗号化プログラムと第２の暗号化プログラムとを上記第１の装置が受信し，上記第１の装置は，第２の暗号化／復号鍵を用いて，上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，受信した上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第３の装置に送信する，暗号化通信方法。

【請求項５０】　コンピュータ装置において，このコンピュータ装置は，他の第１の装置および他の第２の装置と通信手段を介して接続可能であり，さらにこのコンピュータ装置は，上記第２の装置に第１の送信要求を送信し，上記第１の送信要求に応答して上記第２の装置から送信されるデータと上記第１の装置のアドレスとを受信し，上記受信したアドレスにしたがって上記第１の装置に第２の送信要求を送信し，上記第２の送信要求に応答して上記第１の装置から送信される第１の暗号化鍵と，第１の暗号化プログラムと，第２の暗号化プログラムとを受信し，第２の暗号化／復号鍵を用いて上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって，上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第２の装置に送信するものである，コンピュータ装置。

【請求項５１】　請求項１から17に記載の商品を注文する方法をインターネットの通信プログラムと共働して実現するために用いられるバーチャルショップ・サーバの記憶装置に格納すべきデータを記録した記録媒体であって，少なくとも上記クライアント・コンピュータを上記セキュリティサービス・サーバにリンクさせるための上記セキュリティサービス・サーバのアドレスと，暗号化鍵および上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムを上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信させるための上記第２の送信命令とを格納した，サーバが読取可能な記録媒体。

【請求項５２】　復号鍵と，上記復号鍵を用いてデータを復号するための復号プログラムとをさらに格納した，請求項51に記載のサーバ読取可能な記録媒体。

【請求項５３】　上記クライアント・コンピュータから

送信されるユーザ識別子にもとづいて，対応する復号鍵を選んで暗号化されたデータの復号に用いるように上記バーチャルショップ・サーバを制御するためのプログラムをさらに格納した，請求項51または52に記載のサーバ読取可能な記録媒体。

【請求項５４】　請求項１から17に記載の商品を注文する方法をインターネットの通信プログラムと共働して実現するために用いられるセキュリティサービス・サーバの記憶装置に格納すべきプログラムを記録した記録媒体であって，少なくとも暗号化鍵と，上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムと，第２の送信命令を受信したときに上記クライアント・コンピュータに上記暗号化鍵と上記暗号化プログラムとを送信するように上記セキュリティサービス・サーバを制御するためのプログラムを格納した，サーバ読取可能な記録媒体。

【請求項５５】　クライアント・コンピュータから送信されるショップ識別子にもとづいて，対応する暗号化鍵を選んで上記クライアント・コンピュータに送信するように上記セキュリティサービス・サーバを制御するためのプログラムをさらに格納した，請求項54に記載のサーバ読取可能な記録媒体。

【請求項５６】　クライアント・コンピュータから送信されるユーザ識別子にもとづいて，対応する暗号化鍵を選んで上記クライアント・コンピュータに送信するように上記セキュリティサービス・サーバを制御するためのプログラムをさらに格納した，請求項54または55に記載のサーバ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【技術分野】この発明は，通信手段を介して相互に接続可能なコンピュータ間でデータ通信を行うのに適した暗号化処理および復号処理の方法，ならびにシステムに関する。ここで暗号化／復号通信システムとは，暗号化を行う装置を含む通信システム，復号を行う装置を含む通信システム，および暗号化を行う装置と復号を行う装置との両方を含む通信システムを意味する。

【０００２】

【背景技術】文書データ，個人データ等の機密性の高いデータ通信においては，その漏洩を防止するために，データの暗号化が必須である。特に，電子商取引（エレクトロニック・コマース）においては，商品の購買者から受注元（商品の提供者）にネットワークを介して送信されるクレジット・カード番号の悪用や漏洩，送信データ内容の改ざん，いたずらによる注文等を防止するために，データ内容の暗号化や，送信されるデータの認証が不可欠である。

【０００３】電子商取引では，商品の購買者（ユーザ）の側において注文データを暗号化する必要がある。ユーザは暗号化プログラムを何らかの方法で入手して注文データの暗号化処理を行わなければならない。電子商取引の普及のためにはユーザにできるだけ負担をかけないようにすることが好ましい。

【０００４】

【発明の開示】この発明は，多数の者が利用することができるネットワークを通じて，ユーザに負担をかけることなく電子商取引が可能となる商品発注方法およびシステムの提供を目的とする。

【０００５】この発明はまた，安全性の高い商品発注方法およびシステムを提供するものである。

【０００６】この発明はさらに，ユーザの確認が可能な商品発注方法およびシステムを提供する。

【０００７】この発明はさらに，商品発注方法およびシステムを一般化した，ユーザに負担を強いることのない暗号化／復号通信が可能となる方法およびシステムを提供することを目的とする。

【０００８】この発明はさらに，暗号化／復号通信方法およびシステムの安全性を高めることを目的とする。

【０００９】第１の発明による商品注文方法は，クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法である。

【００１０】第１の発明による商品注文システムは，クライアント・コンピュータと，バーチャルショップ・サーバと，セキュリティサービス・サーバとから構成される。クライアント・コンピュータはバーチャルショップ・サーバおよび上記セキュリティサービス・サーバと通信手段を介して接続可能である。このシステムでは，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する。

【００１１】第１の発明による商品の注文方法およびシステムでは，上記セキュリティサービス・サーバに，少なくとも暗号化鍵，および上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムを保持させておく。上記バーチャルショップ・サーバには，復号鍵および上記暗号化プログラムによって暗号化されたデータを復号鍵を用いて復号するための復号プログラム，ならびに商品情報を保持させておく。

【００１２】上記バーチャルショップ・サーバとセキュリティサービス・サーバとが別個のコンピュータ・システムである場合には，好ましくはこれらのサーバを通信手段により相互に接続可能にしておく。通信手段は公衆通信回線でも，専用通信回線でも，単なるケーブルでもよい。上記バーチャルショップ・サーバとセキュリティサービス・サーバとは同一のコンピュータ・システムであってもよい。

【００１３】上記バーチャルショップ・サーバとセキュリティサービス・サーバとが別個のコンピュータである

場合には，復号鍵および復号プログラムを通信回線を介して，またはＦＤ等の媒体を通じて，セキュリティサービス・サーバからバーチャルショップ・サーバにあらかじめ配送しておくことが好ましい。

【００１４】第１の発明による商品注文方法およびシステムでは，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記バーチャルショップ・サーバから上記クライアント・コンピュータに上記商品情報を送信する。上記クライアント・コンピュータでは上記商品情報に基づいて発注する商品情報が決定される。

【００１５】上記クライアント・コンピュータから上記セキュリティサービス・サーバに第２の送信要求を送信すると，この第２の送信要求に応答して，上記セキュリティサービス・サーバは上記クライアント・コンピュータに上記暗号化鍵および上記暗号化プログラムを送信する。

【００１６】上記クライアント・コンピュータは，送信された上記暗号化鍵を用いて上記暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信する。上記バーチャルショップ・サーバは，上記復号鍵を用いて上記復号プログラムにしたがって，暗号化された上記商品発注情報を復号する。

【００１７】第１の発明によると，セキュリティサービス・サーバから暗号化鍵と暗号化プログラムがクライアント・コンピュータに送られるので，クライアント・コンピュータには暗号化プログラムをあらかじめ備える必要がない。また，クライアント・コンピュータからバーチャルショップ・サーバに復号鍵を配送する必要はないので安全性が高まる。

【００１８】上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信される上記暗号化鍵を，上記暗号化プログラムに内蔵させておくと，一層安全性が高まる。

【００１９】上記バーチャルショップ・サーバから上記クライアント・コンピュータに送信される上記商品情報に，上記セキュリティサービス・サーバのアドレスを含ませておけば，上記クライアント・コンピュータは上記アドレスに上記第２の送信要求を送信することができる。すなわち，クライアント・コンピュータにはバーチャルショップ・サーバにアクセスする通信プログラムのみを備えておけばよいことになる。

【００２０】一実施態様では，上記暗号化鍵と上記復号鍵が，データの暗号化と復号に共通に用いられる秘密鍵である。

【００２１】他の実施態様では，上記第１の暗号化プログラムおよび上記第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記暗号化鍵が公開鍵，上記復号鍵が秘密鍵である。公開鍵方式の採用により，安全性がより一層高まる。

【００２２】上記セキュリティサービス・サーバに消去プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記消去プログラムを送信する。上記クライアント・コンピュータにおいて暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信した後，上記消去プログラムにしたがって上記暗号化プログラムおよび上記暗号化鍵のうち少なくともいずれか一つを消去する。これにより，クライアント・コンピュータには暗号化に用いた暗号鍵および暗号化プログラムの少なくともいずれか一方が無くなるので，商品発注情報の送信後は，ユーザがこれらを悪用することができず，安全性が一層高い。

【００２３】バーチャルショップ・サーバが複数台ある場合には，上記暗号化鍵と上記復号鍵との対をバーチャルショップ・サーバごとにそれぞれ異なるものとしておくとよい。

【００２４】上記セキュリティサービス・サーバに，すべての上記暗号化鍵を保持させておく。上記バーチャルショップ・サーバには，それぞれに固有の復号鍵を保持させておく。上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，商品を発注すべき上記バーチャルショップ・サーバを識別するためのショップ識別子を送信する。上記セキュリティサービス・サーバは，送信されたショップ識別子に対応する暗号化鍵を選んで上記クライアント・コンピュータに送信する。

【００２５】これにより，クライアント・コンピュータは複数のうちの一つのバーチャルショップ・サーバと安全な取引を行うことができるようになる。

【００２６】複数のユーザに対応するためには上記暗号化鍵と上記復号鍵との対を複数のユーザごとにそれぞれ異なるものとしておくとよい。

【００２７】上記セキュリティサービス・サーバに，すべてのユーザの暗号化鍵を保持させておく。上記バーチャルショップ・サーバに，そのバーチャルショップ・サーバにアクセスが許されたすべてのユーザの復号鍵を保持させておく。上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，発注を行うユーザを識別するためのユーザ識別子を送信する。上記セキュリティサービス・サーバは，送信されたユーザ識別子に対応する暗号化鍵を選んで上記クライアント・コンピュータに送信する。上記クライアント・コンピュータは，暗号化された上記商品発注情報とともにユーザのユーザ識別子を上記バーチャルショップ・サーバに送信する。上記バーチャルショップ・サーバは，送信されたユーザ識別子に対応する復号鍵を選んで，暗号化された上記商品発注情報を復号する。

【００２８】ユーザ識別子によりクライアント・コンピュータまたはユーザが取引の資格のある正当な者である

ことを判断することが可能となるので，一層取引の安全性が高まる。

【００２９】第１の発明はさらに，上述したクライアント・コンピュータ，およびクライアント・コンピュータによる商品注文方法を提供している。

【００３０】第１の発明はさらに，上述した商品注文する方法をインターネットの通信プログラムと共働して実現するために用いられるバーチャルショップ・サーバの記憶装置に格納すべきデータを記録した記録媒体を提供している。この記録媒体は少なくとも上記クライアント・コンピュータを上記セキュリティサービス・サーバにリンクさせるための上記セキュリティサービス・サーバのアドレスと，暗号化鍵および上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムを上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信させるための上記第２の送信命令とを格納している。これらのアドレスと第２の送信命令とは，クライアント・コンピュータがバーチャルショップ・サーバにアクセスしたときにバーチャルショップ・サーバからクライアント・コンピュータに送信される。

【００３１】第１の発明はさらに上述した商品注文方法をインターネットの通信プログラムと共働して実現するために用いられるセキュリティサービス・サーバの記憶装置に格納すべきプログラムを記録した記録媒体を提供している。この記録媒体は少なくとも暗号化鍵と，上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムと，第２の送信命令を受信したときに上記クライアント・コンピュータに上記暗号化鍵と上記暗号化プログラムとを送信するように上記セキュリティサービス・サーバを制御するためのプログラムを格納している。

【００３２】クライアント・コンピュータから上記の第２の送信命令が送信されたときに，セキュリティサービス・サーバは暗号化鍵と暗号化プログラムとをクライアント・コンピュータに送信する。

【００３３】クライアント・コンピュータに上記セキュリティサービス・サーバから送信される暗号化プログラムを含むプログラムを受信させ，このプログラムにしたがって，ユーザの介入なしに，商品発注情報の暗号化と暗号化された商品発注情報のバーチャルショップ・サーバへの送信とを自動的に行わせてもよい。

【００３４】第２の発明による商品注文方法は，クライアント・コンピュータがバーチャルショップ・サーバおよびセキュリティサービス・サーバと通信手段を介して接続可能であり，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する方法である。

【００３５】第２の発明による商品注文システムは，クライアント・コンピュータと，バーチャルショップ・サーバと，セキュリティサービス・サーバとから構成される。クライアント・コンピュータはバーチャルショップ・サーバおよび上記セキュリティサービス・サーバと通信手段を介して接続可能である。このシステムでは，暗号化通信によって，クライアント・コンピュータからバーチャルショップ・サーバに商品を注文する。

【００３６】第２の発明による商品の注文方法およびシステムでは，上記セキュリティサービス・サーバに，少なくとも暗号化鍵，および上記暗号化鍵を用いてデータを暗号化するための暗号化プログラムを保持させておく。上記セキュリティサービス・サーバに，少なくとも第１の暗号化鍵，第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持させておく。上記バーチャルショップ・サーバに，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，上記第２の暗号化プログラムによって暗号化されたデータを上記第２の暗号化／復号鍵を用いて復号するための第２の復号プログラムおよび商品情報を保持させておく。

【００３７】上記バーチャルショップ・サーバとセキュリティサービス・サーバとが別個のコンピュータ・システムである場合には，好ましくはこれらのサーバを通信手段により相互に接続可能にしておく。通信手段は公衆通信回線でも，専用通信回線でも，単なるケーブルでもよい。上記バーチャルショップ・サーバとセキュリティサービス・サーバとは同一のコンピュータ・システムであってもよい。

【００３８】上記バーチャルショップ・サーバをセキュリティサービス・サーバとが別個のコンピュータである場合には，第１の復号鍵，第１の復号プログラムおよび第２の復号プログラムを通信回線を介して，またはＦＤ等の媒体を通じて，セキュリティサービス・サーバからバーチャルショップ・サーバにあらかじめ配送しておくことが好ましい。

【００３９】第２の発明による商品注文方法およびシステムでは，上記クライアント・コンピュータからの第１の送信要求にもとづいて，上記バーチャルショップ・サーバから上記クライアント・コンピュータに上記商品情報を送信する。上記クライアント・コンピュータでは上記商品情報に基づいて商品発注情報が作成される。

【００４０】上記クライアント・コンピュータから上記セキュリティサービス・サーバに第２の送信要求を送信すると，上記第２の送信要求に応答して，上記セキュリティサービス・サーバは上記クライアント・コンピュータに上記第１の暗号化鍵，上記第１の暗号化プログラムおよび上記第２の暗号化プログラムを送信する。

【００４１】上記クライアント・コンピュータは，上記第２の暗号化／復号鍵を用いて，送信された上記第２の暗号化プログラムにしたがって，商品を発注するための商品発注情報を暗号化し，上記第１の暗号化鍵を用いて

上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，暗号化された上記商品発注情報と，暗号化された上記第２の暗号化／復号鍵とを上記バーチャルショップ・サーバに送信する。

【００４２】上記バーチャルショップ・サーバは，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号化された上記商品発注情報を復号する。

【００４３】第２の発明によると，セキュリティサービス・サーバから第１の暗号化鍵と第１の暗号化プログラムと第２の暗号化プログラムがクライアント・コンピュータに送られるので，クライアント・コンピュータには暗号化プログラムをあらかじめ備える必要がない。また，商品発注情報が第２の暗号化プログラムによって暗号化され，この暗号化に用いた暗号化／復号鍵が第１の暗号化鍵を用いて第１の暗号化プログラムにより暗号化される。鍵は暗号化された上でクライアント・コンピュータからバーチャルショップ・サーバに送られるので取引の安全性が確保される。クライアント・コンピュータからバーチャルショップ・サーバに第１の復号鍵を配送する必要はないので安全性が一層高まる。

【００４４】上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信される上記第１の暗号化鍵を，上記第１の暗号化プログラムに内蔵させておくと，一層安全性が高まる。

【００４５】上記バーチャルショップ・サーバから上記クライアント・コンピュータに送信される上記商品情報に，上記セキュリティサービス・サーバのアドレスを含ませておけば，上記クライアント・コンピュータは上記アドレスに上記第２の送信要求を送信することができる。すなわち，クライアント・コンピュータにはバーチャルショップ・サーバにアクセスする通信プログラムのみを備えておけばよいことになる。

【００４６】一実施態様では上記第１の暗号化プログラムと上記第２の暗号化プログラムとが同じものであり，上記第１の復号プログラムと上記第２の復号プログラムとが同じものである。

【００４７】他の実施態様では上記第１の暗号化鍵と上記第１の復号鍵がデータの暗号化と復号とに共通に用いられる秘密鍵である。

【００４８】さらに他の実施態様では，上記第１の暗号化プログラムおよび第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記第１の暗号化鍵が公開鍵，上記第１の復号鍵が秘密鍵である。

【００４９】上記第２の暗号化／復号鍵は，上記クライアント・コンピュータに入力される入力値であってもよい。または，上記セキュリティサービス・サーバに，乱数生成プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記乱数生成プログラムを送信し，上記クライアント・コンピュータにおいては上記乱数生成プログラムによって乱数を生成し，この生成した乱数を上記第２の暗号化／復号鍵として用いることもできる。

【００５０】上記セキュリティサービス・サーバに消去プログラムを保持させておき，上記第２の送信要求に応答して，上記セキュリティサービス・サーバから上記クライアント・コンピュータに上記消去プログラムを送信する。上記クライアント・コンピュータは，暗号化された上記商品発注情報を上記バーチャルショップ・サーバに送信した後，上記消去プログラムにしたがって上記第１および第２の暗号化プログラム，上記第１の暗号化鍵，上記第２の暗号化／復号鍵，ならびに乱数生成プログラムのうち少なくともいずれか一つを消去する。これにより，クライアント・コンピュータには，暗号化に用いた鍵または暗号化プログラムが商品発注情報の送信後は存在しなくなるので，ユーザがこれらの鍵および暗号化プログラムを悪用することを未然に防止できる。

【００５１】バーチャルショップ・サーバが複数台ある場合には，上記第１の暗号化鍵と上記第１の復号鍵との対をバーチャルショップ・サーバごとにそれぞれ異なるものとしておくとよい。

【００５２】上記セキュリティサービス・サーバに，すべての上記暗号化鍵を保持させておく。上記バーチャルショップ・サーバには，それぞれに固有の復号鍵を保持させておく。上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，商品を発注すべき上記バーチャルショップ・サーバを識別するためのショップ識別子を送信する。上記セキュリティサービス・サーバは，送信されたショップ識別子に対応する暗号化鍵を選んで上記クライアント・コンピュータに送信する。

【００５３】これにより，クライアント・コンピュータは複数のうちの一つのバーチャルショップ・サーバと安全な取引を行うことができるようになる。

【００５４】複数のユーザに対応するためには上記第１の暗号化鍵と上記第１の復号鍵との対を複数のユーザごとにそれぞれ異なるものとしておくとよい。

【００５５】上記セキュリティサービス・サーバに，すべてのユーザの第１の暗号化鍵を保持させておく。上記バーチャルショップ・サーバに，そのバーチャルショップ・サーバにアクセスが許されたすべてのユーザの第１の復号鍵を保持させておく。上記第２の送信要求とともに，上記クライアント・コンピュータから上記セキュリティサービス・サーバに，発注を行うユーザを識別するためのユーザ識別子を送信する。上記セキュリティサービス・サーバは，送信されたユーザ識別子に対応する暗

号化鍵を選んで上記クライアント・コンピュータに送信する。上記クライアント・コンピュータは，暗号化された上記商品発注情報とともにユーザのユーザ識別子を上記バーチャルショップ・サーバに送信する。上記バーチャルショップ・サーバは，送信されたユーザ識別子に対応する第１の復号鍵を選んで，暗号化された上記商品発注情報を復号する。

【００５６】ユーザ識別子によりクライアント・コンピュータまたはユーザが取引の資格のある正当な者であることを判断することが可能となるので，一層取引の安全性が高まる。

【００５７】第２の発明はさらに，上述したクライアント・コンピュータ，およびクライアント・コンピュータによる商品注文方法を提供している。

【００５８】第２の発明はさらに，上述した商品注文する方法をインターネットの通信プログラムと共働して実現するために用いられるバーチャルショップ・サーバの記憶装置に格納すべきデータを記録した記録媒体を提供している。この記録媒体は少なくとも上記クライアント・コンピュータを上記セキュリティサービス・サーバにリンクさせるための上記セキュリティサービス・サーバのアドレスと，上記第１の暗号化鍵，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラムおよび第２の暗号化プログラムを上記セキュリティサービス・サーバから上記クライアント・コンピュータに送信させるための上記第２の送信命令とを格納している。これらのアドレスと第２の送信命令とは，クライアント・コンピュータがバーチャルショップ・サーバにアクセスしたときにバーチャルショップ・サーバからクライアント・コンピュータに送信される。

【００５９】第２の発明はさらに上述した商品注文方法をインターネットの通信プログラムと共働して実現するために用いられるセキュリティサービス・サーバの記憶装置に格納すべきプログラムを記録した記録媒体を提供している。この記録媒体は少なくとも第１の暗号化鍵と，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラムと，第２の暗号化プログラムを，第２の送信命令を受信したときに上記クライアント・コンピュータに送信するように上記セキュリティサービス・サーバを制御するためのプログラムを格納している。

【００６０】クライアント・コンピュータから上記の第２の送信命令が送信されたときに，セキュリティサービス・サーバは第１の暗号化鍵と第１の暗号化プログラムと第２の暗号化プログラムとをクライアント・コンピュータに送信する。

【００６１】上記第１の装置に上記第２の装置から送信される暗号化プログラムを含むプログラムを受信させ，このプログラムにしたがって，ユーザの介入なしに，データの暗号化と暗号化データの第３の装置への送信とを自動的に行わせてもよい。

【００６２】第３の発明は，第１の発明を一般化した暗号化／復号通信方法およびシステムを提供している。

【００６３】第３の発明による暗号化／復号通信方法およびシステムは，第１の装置，第２の装置および第３の装置を含むシステムにおいて，第１の装置が上記第２の装置および上記第３の装置と通信手段を介して接続可能な暗号化／復号通信方法およびシステムに関する。

【００６４】上記第２の装置と上記第３の装置とが別個のコンピュータ・システムの場合には，これらの装置は通信手段により相互に接続可能としておくことが好ましい。

【００６５】上記第２の装置と上記第３の装置とは同一のコンピュータ・システムによっても実現できる。

【００６６】第３の発明による暗号化／復号通信方法は，上記第２の装置に，暗号化鍵と，この暗号化鍵を用いてデータを暗号化するための暗号化プログラムとを保持させておき，上記第１の装置からの送信要求に応答して，上記第２の装置から上記第１の装置に上記暗号化鍵および上記暗号化プログラムを送信し，上記第１の装置は，送信された上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第３の装置に送信するものである。

【００６７】第３の発明による暗号化／復号通信システムにおいては，上記第２の装置は，暗号化鍵と，この暗号化鍵を用いてデータを暗号化するための暗号化プログラムとを保持しており，上記第１の装置からの送信要求に応答して，上記第１の装置に上記暗号化鍵と上記暗号化プログラムとを送信するものであり，上記第１の装置は，上記第２の装置から送信された上記暗号化鍵を用いて上記暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記暗号文データを上記第３の装置に送信するものである。

【００６８】第３の発明によると，第２の装置が暗号化鍵と暗号化プログラムとを第１の装置に送信するので，第１の装置は暗号化鍵と暗号化プログラムを持っていなくても，データを暗号化して暗号文データを生成し，第３の装置に送ることができる。

【００６９】好ましい実施態様では，上記第３の装置に，復号鍵と，上記暗号化プログラムによって暗号化されたデータを上記復号鍵を用いて復号するための復号プログラムとを保持させておく。上記第３の装置において，上記復号鍵を用いて上記復号プログラムにしたがって，上記第１の装置から送信された暗号文データを復号する。

【００７０】第１の装置から第３の装置に復号鍵を送る必要がないので安全性が高まる。

【００７１】さらに好ましい実施態様においては，上記第３の装置は，上記第１の装置からの要請に応じて，上

記第２の装置のアドレスを含むデータを上記第１の装置に送信する。上記第１の装置は上記アドレスに上記送信要求を送信する。

【００７２】第１の装置は第３の装置をアクセスできる通信プログラムさえ備えておけば，上記アドレスにしたがって第２の装置に送信要求を送ることができる。

【００７３】一実施態様においては，上記暗号化鍵と上記復号鍵がデータの暗号化と復号に共通に用いられる秘密鍵である。

【００７４】他の実施態様においては，上記暗号化プログラムおよび上記復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記暗号化鍵が公開鍵，上記復号鍵が秘密鍵である。

【００７５】さらに好ましい実施態様においては，上記第２の装置に消去プログラムを保持させておき，上記送信要求に応答して，上記第２の装置から上記第１の装置に上記消去プログラムを送信する。上記第１の装置は，上記暗号文データを上記第３の装置に送信した後，上記消去プログラムにしたがって上記暗号化プログラムおよび上記暗号化鍵のうち少なくともいずれか一つを消去する。

【００７６】第１の装置の暗号化鍵または暗号化プログラムは暗号文データの送信後，消去されるから，第１の装置において暗号化処理の悪用が未然に防止される。

【００７７】第３の発明はさらに，第１の装置から第３の装置にデータを暗号化して送信する暗号化通信方法，および第１の装置からなるコンピュータ・システム，第２の装置を制御するためのプログラムを記憶した媒体，および第３の装置を制御するためのプログラムを記憶した媒体を提供している。

【００７８】第４の発明は，第２の発明を一般化した暗号化／復号通信方法およびシステムを提供している。

【００７９】第４の発明による暗号化／復号通信方法およびシステムは，第１の装置，第２の装置および第３の装置を含むシステムにおいて，第１の装置が上記第２の装置および上記第３の装置と通信手段を介して接続可能な暗号化／復号通信方法およびシステムに関する。

【００８０】上記第２の装置と上記第３の装置とが別個のコンピュータ・システムの場合には，これらの装置は通信手段により相互に接続可能としておくことが好ましい。

【００８１】上記第２の装置と上記第３の装置とは同一のコンピュータ・システムによっても実現できる。

【００８２】第４の発明による暗号化／復号通信方法は，上記第２の装置に，第１の暗号化鍵，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持させておき，上記第１の装置からの送信要求に応答して，上記第２の装置から上記第１の装置に上記第１の暗号化鍵，上記第１の暗号化プログラムおよび上記第２の暗号化プログラムとを送信し，上記第１の装置は，上記第２の暗号化／復号鍵を用いて，送信された上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記第１の暗号化鍵を用いて上記第１の暗号化プログラムにしたがって上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第３の装置に送信するものである。

【００８３】第４の発明による暗号化／復号通信システムは，上記第２の装置は，第１の暗号化鍵，上記第１の暗号化鍵を用いてデータを暗号化するための第１の暗号化プログラム，および第２の暗号化／復号鍵を用いてデータを暗号化するための第２の暗号化プログラムを保持しており，上記第１の装置からの送信要求に応答して，上記第１の装置に上記第１の暗号化鍵と上記第１の暗号化プログラムと上記第２の暗号化プログラムとを送信するものであり，上記第１の装置は，上記第２の暗号化／復号鍵を用いて，上記第２の装置から送信された上記第２の暗号化プログラムにしたがって，データを暗号化して暗号文データを生成し，上記第１の暗号化鍵を用いて，上記第１の暗号化プログラムにしたがって，上記第２の暗号化／復号鍵を暗号化し，上記暗号文データと暗号化された上記第２の暗号化／復号鍵とを上記第３の装置に送信するものである。

【００８４】第４の発明によると，第２の装置が第１の暗号化鍵と第１の暗号化プログラムと第２の暗号化プログラムとを第１の装置に送信するので，第１の装置はこれらの暗号化鍵と暗号化プログラムを持っていなくても，データを暗号化して暗号文データを生成し，第３の装置に送ることができる。また，データを暗号化するのに用いる第２の暗号化／復号鍵も暗号化されるので安全性が一層高まる。

【００８５】好ましい実施態様では，上記第３の装置に，第１の復号鍵，上記第１の暗号化プログラムによって暗号化されたデータを上記第１の復号鍵を用いて復号するための第１の復号プログラム，および上記第２の暗号化プログラムによって暗号化されたデータを上記第２の暗号化／復号鍵を用いて復号するための第２の復号プログラムを保持させておく。上記第３の装置は，上記第１の復号鍵を用いて上記第１の復号プログラムにしたがって，暗号化された上記第２の暗号化／復号鍵を復号し，復号された上記第２の暗号化／復号鍵を用いて上記第２の復号プログラムにしたがって，暗号文データを復号する。

【００８６】第１の装置から第３の装置に第１の復号鍵を送る必要がないので安全性が高まる。

【００８７】さらに好ましい実施態様においては，上記第３の装置は，上記第１の装置からの要請に応じて，上記第２の装置のアドレスを含むデータを上記第１の装置

に送信する。上記第１の装置は上記アドレスに上記送信要求を送信する。

【００８８】第１の装置は第３の装置をアクセスできる通信プログラムさえ備えておけば，上記アドレスにしたがって第２の装置に送信要求を送ることができる。

【００８９】一実施態様においては，上記第１の暗号化鍵と上記第１の復号鍵がデータの暗号化と復号に共通に用いられる秘密鍵である。

【００９０】他の実施態様においては，上記第１の暗号化プログラムおよび上記第１の復号プログラムが公開鍵方式の暗号化プログラムおよび復号プログラムであり，上記第１の暗号化鍵が公開鍵，上記復号鍵が秘密鍵である。

【００９１】一実施態様では，上記第１の暗号化プログラムと上記第２の暗号化プログラムとが同じものであり，上記第１の復号プログラムと上記第２の復号プログラムとが同じものである。

【００９２】上記第２の暗号化／復号鍵として，上記第１の装置に入力される入力値を用いることができる。または，上記第２の装置に，乱数生成プログラムを保持させておき，上記第２の送信要求に応答して，上記第２の装置から上記第１の装置に上記乱数生成プログラムを送信し，上記第１の装置は上記乱数生成プログラムによって乱数を生成し，この生成した乱数を上記第２の暗号化／復号鍵として用いてもよい。

【００９３】さらに好ましい実施態様では上記第２の装置に消去プログラムを保持させておき，上記第２の送信要求に応答して，上記第２の装置から上記第１の装置に上記消去プログラムを送信し，上記第１の装置は，暗号化された上記商品発注情報を上記第３の装置に送信した後，上記消去プログラムにしたがって上記第１および第２の暗号化プログラム，上記第１の暗号化鍵，上記第２の暗号化／復号鍵，ならびに乱数生成プログラムのうち少なくともいずれか一つを消去する。

【００９４】第１の装置の第１の暗号化鍵，第２の暗号化／復号鍵，第１もしくは第２の暗号化プログラムまたは乱数生成プログラムは暗号文データの送信後，消去されるから，第１の装置において暗号化処理の悪用が未然に防止される。

【００９５】第４の発明はさらに，第１の装置から第３の装置にデータを暗号化して送信する暗号化通信方法，および第１の装置からなるコンピュータ・システム，第２の装置を制御するためのプログラムを記憶した媒体，および第３の装置を制御するためのプログラムを記憶した媒体を提供している。

【００９６】

【実施例】

第１実施例

図１は第１実施例のＥＣ（エレクトロニック・コマース）システムの全体的構成を示している。

【００９７】ＥＣシステムは，商品の購買者であるユーザの有するクライアント・コンピュータ10と，商品情報を配信し，ユーザからの商品の注文を受け付ける販売者（販売会社）の有するバーチャルショップ・サーバＳ11と，クライアント・コンピュータ10からバーチャルショップ・サーバＳ11に送信される商品の発注情報を暗号化する暗号化プログラムおよび暗号化された発注情報を復号する復号プログラム等を提供する管理者（管理会社）の有するセキュリティサービス・サーバＣ12と，これらのコンピュータ，サーバ間の通信の媒体となるネットワーク13とから構成されている。

【００９８】ネットワーク13は既存のまたは将来敷設される公衆回線または専用回線であり，たとえばTCP/IP（TransmissionControl Protocol／Internet Protocol），HTTP（HyperText Transfer Protocol）などの通信プロトコルを用いてデータ伝送が可能なものである。クライアント・コンピュータ10，サーバＳ11およびサーバＣ12もまたこれらの通信プロトコルを利用可能なコンピュータを含み，ネットワーク13を通じて相互にデータ通信を行うことができる。

【００９９】クライアント・コンピュータ10は，たとえばパーソナル・コンピュータであり，表示装置（ＣＲＴ表示装置等），入力装置（キーボード，マウス等），記憶装置（磁気ディスク記憶装置，光ディスク記憶装置等）および通信装置（モデム等）を含む。サーバＳ11およびサーバＣ12は，たとえばワーク・ステーションであり，コンピュータ10と同様に，表示装置，入力装置，記憶装置および通信装置を含む。

【０１００】バーチャルショップ・サーバＳ11を所有する販売者とセキュリティサービス・サーバＣ12を所有する管理者とは，同一人（同一会社）であってもよいし，異なる人（異なる会社）であってもよい。また，バーチャルショップ・サーバＳ11とセキュリティサービス・サーバＣ12は同じコンピュータ・システムで実施することもできるし，異なるコンピュータ・システムでもよい。後者の場合には，バーチャルショップ・サーバＳ11とセキュリティサービス・サーバＣ12とは公衆回線，専用回線，または単なるケーブルもしくはバスによって接続されよう。

【０１０１】ＥＣシステムにおいてユーザに提供される商品情報（複数の商品について，それらの外観，規格，性能，効能，価格等）は，バーチャルショップ・サーバＳ11の記憶装置に記憶されている。ここで，商品にはサービス（役務）も含まれるものとする。ユーザは，ネットワーク13を介してクライアント・コンピュータ10をバーチャルショップ・サーバＳ11に接続し，バーチャルショップ・サーバＳ11の記憶装置に記憶されている商品情報（ホーム・ページ）を受信して参照（閲覧）することができる。商品情報は一般に文字データ，画像データによって構成され，これらがクライアント・コンピュータ

10の表示装置の表示画面に表示される。

【０１０２】このような情報閲覧の手段として，インターネットにおいて構築されたｗｗｗ（World Wide Web）が知られている。ユーザがクライアント・コンピュータ10をインターネットを介してｗｗｗサーバに接続（アクセス）すると，接続先のｗｗｗサーバの記憶装置に記憶されているホームページ（文字データ，画像データ等）がクライアント・コンピュータ10に送信される。この場合には，ｗｗｗサーバはバーチャルショップ・サーバＳ11の一部を構成することになる。クライアント・コンピュータ10からｗｗｗサーバに向けてデータを送信することも可能である。

【０１０３】ＥＣシステムにおいて，ユーザは商品の発注をネットワーク13を介して行うことができる。ユーザが商品を発注する最も基本的な形態について説明する。ユーザは，クライアント・コンピュータ10に，入力装置を用いて発注情報（たとえば，ユーザの住所，氏名，電話番号，希望する商品の商品番号，クレジットカードの番号等）を入力する。発注情報を入力した後，ユーザはクライアント・コンピュータ10に商品の発注の最終確認を入力する。最終確認を入力すると，クライアント・コンピュータ10は，自動的にセキュリティサービス・サーバＣ12に接続される。セキュリティサービス・サーバＣ12は，最終確認を行ったクライアント・コンピュータ10に，暗号化プログラムと暗号化鍵とを送信する。クライアント・コンピュータ10は受信した暗号化プログラムを実行し，暗号化鍵を用いて発注情報の暗号化を行う。クライアント・コンピュータ10によって暗号化された発注情報は，クライアント・コンピュータ10からバーチャルショップ・サーバＳ11に送信される。

【０１０４】バーチャルショップ・サーバＳ11には，セキュリティサービス・サーバＣ12からネットワーク13を通じて，またはその他の手段によって，あらかじめ復号プログラムおよび復号鍵が配送され（後述するように種々の配送方法がある），バーチャルショップ・サーバＳ11の記憶装置に記憶されている。バーチャルショップ・サーバＳ11に配送される復号プログラムは，クライアント・コンピュータ10が実行する暗号プログラムの暗号アルゴリズムとセットになったものである。バーチャルショップ・サーバＳ11は暗号化発注情報を受信すると，復号プログラムを実行し，復号鍵を用いて受信した暗号化発注情報を復号する。暗号化発注情報はもとの発注情報（平文）に復号される。

【０１０５】クライアント・コンピュータ10の記憶装置，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12の記憶装置にはそれぞれオペレーティング・システム（ＯＳ），および通信ソフトウエアが格納されている。クライアント・コンピュータ10は，ＯＳおよび通信ソフトウエアに基づいて，発注の最終確認のセキュリティサービス・サーバＣ12への送信，サーバＣ12から受信した暗号化プログラムの実行，暗号化発注情報のバーチャルショップ・サーバＳ11への送信を行う。バーチャルショップ・サーバＳ11は，ＯＳおよび通信ソフトウエアに基づいて，商品情報のクライアント・コンピュータ10への送信，暗号化発注情報のクライアント・コンピュータ10からの受信，復号プログラムの実行を行う。セキュリティサービス・サーバＣ12は，ＯＳおよび通信ソフトウエアに基づいて，クライアント・コンピュータ10からの発注の最終確認の受信，クライアント・コンピュータ10への暗号化プログラムおよび暗号化鍵の送信を行う。

【０１０６】図２(A) は，暗号化プログラムと復号プログラムにそれぞれ含まれている暗号（復号）アルゴリズムの一例を示している。この暗号アルゴリズムの例は，ＤＥＳ（Data Encryption Standard）のアルゴリズムを変形したものである（以下，ＤＥＳ型暗号という）。ＤＥＳ型暗号では一般に64ビットの平文および56ビットの鍵が用いられる。ここでは簡単化のため８ビットの平文および12ビットの鍵が用いられているものとする。

【０１０７】Ｓボックス21～24は図２(B) に示されている換字（変換）の対応表にしたがって，入力データを出力データに換字する。たとえば，入力データが１（10進数）の場合は，出力データは14（10進数）に換字される。演算子25～32は，入力される２つのデータの排他的論理和演算を行い，その結果を出力する。

【０１０８】暗号化の対象である８ビットの平文は，上位４ビット・データＬ1 （＝0100）と下位４ビット・データＲ1 （＝1101）とに分割される。データＬ1 は演算子25に，データＲ1 （＝Ｌ2 ）は演算子29および26に入力される。12ビットの鍵Ｋ（＝001010000110）は，上位から３ビットずつの第１～４ブロックの４つのブロックに分けられる。第１ブロック（＝001 ）および第３ブロック（＝000 ）には，１ビット・データの１が各ブロックの最上位ビットとしてそれぞれ加えられる。第２ブロック（＝010 ）および第４ブロック（＝110 ）には，１ビット・データの０が各ブロックの最上位ビットとしてそれぞれ加えられる。その結果，鍵Ｋは４ビット・データＫ1 （＝1001），Ｋ2 （＝0010），Ｋ3 （＝1000）およびＫ4（＝0110）に変換される。データＫ1 は演算子29に，データＫ2 は演算子30に，データＫ3 は演算子31に，データＫ4 は演算子32にそれぞれ入力される。

【０１０９】第１段の処理では，データＲ1 とＫ1 との排他的論理和が，演算子29において求められる。この演算結果は，Ｓボックス21において変換（換字）される。そして，変換されたデータとデータＬ1 との排他的論理和が，演算子25において求められる。この結果のデータＲ2 は演算子30および27に入力される。

【０１１０】第２段においても，データＲ2 ，Ｋ2 およびＬ2 について，第１段と同様の処理が行われる。第３段および第４段においても，データＲ3 ，Ｋ3 およびＬ

3 ならびにデータＲ４，Ｋ4 およびＬ4 について，第１段と同様の処理が行われる。

【０１１１】第１段～第４段の処理によって，８ビットの暗号文が生成される。演算子28の出力データが，８ビットの暗号文の上位４ビット・データ（Ｌ＝1001）となる。演算子27の出力データがＲ4 が８ビットの暗号文の下位４ビット・データ（Ｒ＝0111）となる。このように平文（発注情報）は８ビットずつ順次処理されていき，暗号文が８ビットずつ順次生成されていく。

【０１１２】８ビットの暗号文を８ビットの平文に復号する場合には，８ビットの暗号文が上位４ビット（Ｌ1 ）と下位４ビット（Ｒ1 ）のデータに分割される。この上位４ビット・データは演算子25に，下位４ビット・データは演算子29および26にそれぞれ入力される。復号鍵（暗号鍵Ｋ）と同じものが，暗号化処理と同様に３ビットずつに分割され，データＫ1 からＫ4 が作成される。そして，データＫ4 が演算子29に，データＫ3 が演算子30に，データＫ2 が演算子31に，データＫ1 が演算子32にそれぞれ入力される。これらの入力データに第１段～第４段の処理が行われ，平文８ビットが生成される。このように復号時には，暗号文が８ビットずつ順次処理されていき，平文が８ビットずつ順次生成されていく。

【０１１３】暗号および復号に用いられるアルゴリズムには，このＤＥＳのアルゴリズムのほかにＦＥＡＬ（Fast Encyption ALgorithm）等の他のアルゴリズムを用いることもできる。またアルゴリズムとして対称暗号系と非対称暗号系（べき乗剰余型，ナップザック型等）の別およびブロック暗号とストリーム暗号（バーナム暗号，ＮＦＳＲ等）の別を問わない。さらに，公開鍵方式暗号化（復号）方法も利用可能である。

【０１１４】これらの暗号化／復号処理は，ソフトウェア（プログラム）によって実現することができる。プログラムによって実現した場合には，このプログラムは，コンピュータ10によって実行される暗号化プログラムの一部およびバーチャル・ショップのサーバＳ11によって実行される復号プログラムの一部として組み込まれる。

【０１１５】図３は第１実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12間のデータ（プログラムを含む）の流れと，クライアント・コンピュータ10における暗号化処理と，バーチャルショップ・サーバＳ11における復号処理の様子を示している。図４はクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。

【０１１６】セキュリティサービス・サーバＣ12の記憶装置には，暗号化鍵41，復号鍵42，暗号化プログラムおよび復号プログラムが記憶されている。たとえば，原始多項式Ｆ（ｘ）＝ｘｐ＋ｘｑ＋１（ｐ，ｑは整数）に基づく乱数を生成し，これを暗号化鍵41および復号鍵42とする。生成された乱数をさらに暗号化して生成された値を暗号化鍵41および復号鍵42として用いてもよい。暗号化鍵41を用いて暗号化プログラムにしたがって暗号化されたデータは，復号鍵42を用いて復号プログラムにしたがって復号される。この暗号化プログラムと復号プログラムとはセットになっているものである。

【０１１７】はじめに，復号鍵42と復号プログラムがセキュリティサービス・サーバＣ12からバーチャルショップ・サーバＳ11に配送される（ステップ101 ）。

【０１１８】セキュリティサービス・サーバＣ12からバーチャルショップ・サーバＳ11への復号鍵42と復号プログラムの配送は，たとえば復号鍵42と復号プログラムとを記録した磁気ディスクの郵送（または人による配達）によって行われる。復号鍵42のみを磁気ディスクに記録して郵送し，復号プログラムはネットワーク13を通じてバーチャルショップ・サーバＳ11に送信してもよい。復号プログラムと復号鍵42とをネットワーク13を通してセキュリティサービス・サーバＣ12からバーチャルショップ・サーバＳ11に送信することもできる。この場合，復号鍵42を内蔵した復号プログラムをネットワーク13を通じてバーチャルショップ・サーバＳ11に送信することが望ましい。復号鍵42は復号処理において重要な役割を果たすので，鍵のみを単独でネットワーク13を通じて送信しないことが望ましい。

【０１１９】復号プログラムおよび復号鍵42（または復号鍵42のみ）を格納した磁気ディスクを郵送（配達）した場合には，郵送した磁気ディスクをバーチャルショップ・サーバＳ11に読み込ませ，復号プログラムと復号鍵42とをバーチャルショップ・サーバＳ11の記憶装置に記憶させる。復号プログラム（または復号鍵を内蔵した復号プログラム）がネットワーク13を通じて送信された場合には，復号プログラムはバーチャルショップ・サーバＳ11の通信装置を通して記憶装置に記憶される。このように，復号プログラムと復号鍵42とは，ＥＣシステムの実際の稼動に先だって，バーチャルショップ・サーバＳ11の記憶装置に記憶される。後述するように，復号プログラムと復号鍵42とは，暗号化発注情報の復号処理に用いられる。もっとも，クライアント・コンピュータ10からセキュリティサービス・サーバＣ12に送信命令が送られたときに，その都度，セキュリティサービス・サーバＣ12が復号プログラムと復号鍵42とをバーチャルショップ・サーバＳ11に送信するようにしてもよい。

【０１２０】ユーザは，クライアント・コンピュータ10を用いてバーチャルショップ・サーバＳ11に商品情報の送信を要求する（ステップ102 ）。

【０１２１】ｗｗｗの場合，ユーザは情報閲覧用の通信ソフトウエア（一般に，ブラウザと呼ばれる）を起動し，入力装置からｗｗｗサーバのURL （Uniform Resource Locator）を入力（指定）する。するとｗｗｗサーバ

として働くバーチャルショップ・サーバＳ11から商品情報を含むホームページがクライアント・コンピュータ10に送信される。ｗｗｗサーバがバーチャルショップ・サーバＳ11の一部を構成する態様では，サーバＳ11のURLを指定すると，ｗｗｗサーバに記憶された商品情報を含むホームページがクライアント・コンピュータ10に送信される（ステップ103 ）。ｗｗｗにおいて，バーチャルショップ・サーバＳ11とクライアント・コンピュータ10との間のデータの送受信は，HTTP（HyperText Transfer Protocol） と呼ばれる通信プロトコルに従う。

【０１２２】表示装置の表示画面に表示されるホームページは，HTML（HyperText Markup Language ）と呼ばれる記述形式に従って記述されたHTMLファイルに基づく。クライアント・コンピュータ10にHTMLファイルが読み込まれると，通信ソフトウェア（ブラウザ）はそのHTMLファイルを解釈し，HTMLファイルの記述に従って画像データ，文字データ等を表示装置の表示画面に表示する。

【０１２３】クライアント・コンピュータ10がバーチャルショップ・サーバＳ11から送信されたHTMLファイルを読み込むと，クライアント・コンピュータ10の表示装置の表示画面には，商品の写真，機能，性能，価格等が表示される。ユーザは表示させるべき商品を順次選びながら，または画面をスクロールしながら所望の商品を探し出す。さらに，クライアント・コンピュータ10の表示画面には，氏名，住所および電話番号の入力欄，購入を希望する商品の商品名（または商品番号）の入力欄，クレジットカード番号の入力欄，商品の送付先（住所）の入力欄，注文ボタン，その他バーチャル・ショップが必要とする項目の入力欄が表示される（ステップ104 ）。

【０１２４】ユーザは氏名，住所，電話番号，購入を希望する商品の商品番号，クレジット・カード番号，商品の送付先等（以下，これらを発注情報という）を，入力装置を用いてクライアント・コンピュータ10に入力する。入力された発注情報は，クライアント・コンピュータ10の内部メモリ（RAM 等）に記憶される。発注情報を入力した後，ユーザは商品の注文の最終確認として，画面上に表示された注文ボタン（アイコン）をクリックする（ステップ105 ）。

【０１２５】注文ボタンをクリックすると，クライアント・コンピュータ10はセキュリティサービス・サーバＣ12に自動的に接続される。セキュリティサービス・サーバＣ12のURL ，暗号化プログラムが格納されたサーバＣ12の記憶装置のディレクトリ，および暗号化プログラムの送信命令を含むリンク情報を，バーチャルショップ・サーバＳ11のホーム・ページ（HTMLファイル）の注文ボタンに対応する部分に記述しておく。クライアント・コンピュータ10からセキュリティサービス・サーバＣ12に最終確認情報（送信命令）が送られ，これに応答してセキュリティサービス・サーバＣ12は，クライアント・コンピュータ10に暗号化鍵41を内蔵した暗号化プログラムを送信する（ステップ106 ）。

【０１２６】暗号化鍵41は，好ましくは暗号化プログラムに内蔵された状態でクライアント・コンピュータ10に送信される。暗号化鍵41を暗号化プログラムに内蔵する作業は，クライアント・コンピュータ10からセキュリティサービス・サーバＣ12に送信命令が送信されたとき（ユーザが注文ボタンをクリックしたとき）にセキュリティサービス・サーバＣ12によって行われる。あらかじめ暗号化鍵41を内蔵した暗号化プログラムをセキュリティサービス・サーバＣ12の記憶装置に記憶させておいてもよい。

【０１２７】クライアント・コンピュータ10は暗号化鍵41を内蔵した暗号化プログラムを受信すると，それを記憶装置に記憶する。暗号化プログラムの起動命令が，ユーザによって入力装置からクライアント・コンピュータ10に入力されると，暗号化プログラムが記憶装置から読み出され，クライアント・コンピュータ10の内部メモリ（RAM 等）に格納される。そして，クライアント・コンピュータ10は，暗号化プログラムを実行する。

【０１２８】クライアント・コンピュータ10の内部メモリに記憶されている発注情報（氏名，クレジットカード番号等）は，暗号化鍵41を用いて暗号化される（ステップ107 ）。暗号化処理には，上述した暗号化アルゴリズムの一つが用いられる。ユーザは，その後，入力装置を用いて，暗号化発注情報をバーチャルショップ・サーバＳ11に送信する送信命令をクライアント・コンピュータ10に入力する。暗号化発注情報はネットワーク13を通じてバーチャルショップ・サーバＳ11に送信される（ステップ108 ）。

【０１２９】バーチャルショップ・サーバＳ11は暗号化発注情報を受信すると，それを内部メモリに記憶する。セキュリティサービス・サーバＣ12からあらかじめ配送されている復号プログラムと復号鍵42が記憶装置から読み出され，サーバＳ11の内部メモリに格納される。そして，サーバＳ11は復号プログラムを実行する。暗号化発注情報は復号鍵42を用いて復号され，もとの発注情報（平文）が生成される。バーチャルショップ・サーバＳ11は商品の注文を受注したことになる（ステップ109 ）。

【０１３０】ネットワーク13を通してクライアント・コンピュータ10からバーチャルショップ・サーバＳ11に送信される個人的な情報（氏名，住所，電話番号等）やクレジット・カードの番号は，暗号化されて送信されるので，クレジット・カード番号の盗用や，発注情報の改ざんを防ぐことができ，安全性の高い取引が可能となる。また，暗号化処理を必要とするときにセキュリティサービス・サーバＣ12からクライアント・コンピュータ10に暗号化プログラムと暗号化鍵とが送信されるので，ユーザ側は暗号化プログラムや暗号化鍵を用意しておく必要がない。

【０１３１】セキュリティサービス・サーバ12Ｃからクライアント・コンピュータ10に暗号化鍵を内蔵した暗号化プログラムを送信するとともに，ホーム・ページ（HTMLファイル）を送信するようにしてもよい。このHTMLファイルに，暗号化プログラムの実行命令文と，バーチャルショップ・サーバＳ11のURL と，暗号化発注情報の送信命令文と，これらの命令の実行に関する説明を記述しておく。これにより，暗号化発注情報のバーチャルショップ・サーバＳ11への送信をユーザに指示するための案内が，クライアント・コンピュータ10の表示装置の表示画面に表示される。ユーザは，表示画面の表示にしたがうことによって，暗号化プログラムの実行と，暗号化発注情報のバーチャルショップ・サーバＳ11への送信とを行うことができる。

【０１３２】セキュリティサービス・サーバＣ12からクライアント・コンピュータ10に送信される暗号化プログラムをHTMLファイルに組込まれた自己実行型プログラムにより実現すると一層好ましい。自己実行型プログラミング言語には，「Java」や，「ActiveX」 などが知られている。自己実行型プログラミング言語による暗号化プログラムおよび送信命令をHTMLファイルに組込んでおけば，このHTMLファイルを受信したときに，既に入力されている発注情報を自動的に暗号化して暗号化発注情報を生成したのち，その暗号化発注情報をバーチャルショップ・サーバＳ11に自動的に送信する。暗号化プログラムの起動命令や，暗号化発注情報の送信命令をクライアント・コンピュータ10に入力する必要がないので，ユーザは発注情報の暗号化処理を認識することなく，発注情報を暗号化してバーチャルショップ・サーバＳ11に送信することができる。

【０１３３】図５は，バーチャルショップ・サーバＳ11が複数存在する場合におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12間のデータ（プログラムを含む）の流れと，クライアント・コンピュータ10における暗号化処理およびバーチャルショップ・サーバＳ11における復号処理の様子を示している。図６は，バーチャルショップ・サーバＳ11が複数存在する場合のクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。図６に示すステップ101 からステップ104 およびステップ106 からステップ109 は基本的には図４に示すものと同じである。図４に示すものと異なる点についてのみ説明する。

【０１３４】複数のバーチャルショップ・サーバＳ11がネットワーク13に接続されている場合，セキュリティサービス・サーバＣ12はバーチャルショップ・サーバＳ11ごとに固有の暗号化鍵41と復号鍵42（符号Ａ，Ｂ，で区別する）を生成し，復号鍵42とショップ識別子を各バーチャルショップ・サーバＳ11にそれぞれ配送する（ステップ101 ）。ショップ識別子はバーチャルショップ・サーバＳ11を区別するためのものである。バーチャルショップ・サーバＳ11はそのショップ識別子を商品情報（ホームページ）の中にいれておく。商品情報とともにショップ識別子がバーチャルショップ・サーバＳ11からクライアント・コンピュータ10に送信される（ステップ103，104）。ユーザが注文ボタンをクリックすると，暗号化プログラムの送信要求（命令）とバーチャルショップ・サーバＳ11のショップ識別子が，セキュリティサービス・サーバＣ12に送信される（ステップ105Ａ）。

【０１３５】セキュリティサービス・サーバＣ12は，受信したショップ識別子にもとづいて，バーチャルショップ・サーバＳ11ごとに生成された複数の暗号化鍵41の中から，商品の発注が行われたバーチャルショップ・サーバＳ11に固有の暗号化鍵41を選び出す。そして，選び出した暗号化鍵41を暗号化プログラムに内蔵し，クライアント・コンピュータ10に送信する（ステップ106）。

【０１３６】第２実施例

図７は第２実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12間のデータ（プログラムを含む）の流れと，クライアント・コンピュータ10における暗号化処理と，バーチャルショップ・サーバＳ11における復号処理の様子を示している。図８はクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。ステップ102 ～ステップ105 の処理は，第１実施例（図４）と同じなので，重複した説明を避ける。第２実施例では，第１実施例における「暗号化鍵」および「復号鍵」をそれぞれ「管理鍵41」，「管理鍵42」と呼ぶことにする。

【０１３７】セキュリティサービス・サーバＣ12はバーチャルショップ・サーバＳ11にあらかじめ，管理鍵42と通信鍵復号プログラムと発注情報復号プログラムとを配送しておく（ステップ110 ）。

【０１３８】ユーザが注文ボタンをクリックすると，暗号化プログラムの送信要求がセキュリティサービス・サーバＣ12に送信される（ステップ105 ）。送信要求を受信したセキュリティサービス・サーバＣ12は，乱数生成プログラムと，発注情報暗号化プログラムと，管理鍵41を内蔵した通信鍵暗号化プログラムとをクライアント・コンピュータ10に送信する（ステップ111 ）。

【０１３９】はじめに，乱数生成プログラムがクライアント・コンピュータ10の記憶装置から内部メモリに読み出されて実行される（ステップ112 ）。乱数生成プログラムによって生成された乱数を通信鍵43とする。通信鍵43は，後述するように，暗号化処理と復号処理の両方に用いられる。

【０１４０】発注情報暗号化プログラムには暗号化鍵は内蔵されていない。発注情報暗号化プログラムがクライ

アント・コンピュータ10の記憶装置から内部メモリに読み出される。通信鍵43を用いて発注情報暗号化プログラムによって，ユーザによって入力され内部メモリに記憶されている発注情報が暗号化される（ステップ113 ）。暗号化処理により生成された暗号化発注情報は，中間データとしてクライアント・コンピュータ10の内部メモリに記憶される。

【０１４１】さらに，管理鍵41を内蔵した通信鍵暗号化プログラムが，記憶装置から内部メモリに読み出されて実行される。これにより，発注情報の暗号化に用いられた通信鍵43は管理鍵41を用いて暗号化される（ステップ114 ）。暗号化された通信鍵43を暗号化通信鍵44とする。

【０１４２】その後，中間データとして内部メモリに記憶されている暗号化発注情報と，暗号化通信鍵44とがバーチャルショップ・サーバＳ11に送信される（ステップ115）。

【０１４３】）。バーチャルショップ・サーバＳ11に送信された暗号化発注情報と暗号化通信鍵44とは，ともに内部メモリに記憶される。バーチャルショップ・サーバＳ11の記憶装置にあらかじめ記憶されている管理鍵42と通信鍵復号プログラムとがバーチャルショップ・サーバＳ11の記憶装置から内部メモリに読み出され，この管理鍵42を用いて通信鍵復号プログラムが実行される。

【０１４４】はじめに，暗号化通信鍵44が管理鍵42を用いて通信鍵復号プログラムにしたがって復号され，通信鍵43が得られる（ステップ116 ）。暗号化通信鍵44の復号に用いられる管理鍵42は，通信鍵43の暗号化に用いられた管理鍵41（ステップ114参照）と同じものである。

【０１４５】続いて，暗号化発注情報が，復号された通信鍵43を用いて発注情報復号プログラムにしたがって復号され，発注情報（平文）が得られる（ステップ117 ）。

【０１４６】発注情報の暗号化に用いる通信鍵43を，管理鍵41を用いて暗号化することによって，第三者による暗号化発注情報の解読は困難なものになる。クライアント・コンピュータ10において乱数生成プログラムを用いて複数の乱数（通信鍵：第１，第２，第３・・・の通信鍵という）を生成し，発注情報の暗号化に用いた第１の通信鍵を第２の通信鍵で暗号化し，さらにこの暗号化された第２の通信鍵を第３の通信鍵で暗号化する・・・というように，通信鍵の暗号化を多重に行ってもよい（最後に第ｎの通信鍵が管理鍵で暗号化される）。第三者による発注情報の解読はさらに困難になる。

【０１４７】複数のバーチャルショップ・サーバＳ11が存在する場合にも第２実施例は適用できる。上述したようにショップ識別子が用いられる。

【０１４８】第３実施例

図９は第３実施例のＥＣ（エレクトロニック・コマース）システムの全体的構成を示している。複数のクライアント・コンピュータ10がネットワーク13に接続されている。

【０１４９】図10は，第３実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12間のデータ（プログラムを含む）の流れと，クライアント・コンピュータ10における暗号化処理と，バーチャルショップ・サーバＳ11における復号処理の様子を示している。図11は，クライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。第３実施例において，複数のクライアント・コンピュータ10はそれぞれ同じ処理を行うので，一台のクライアント・コンピュータ（このコンピュータをコンピュータ（001 ）とする）の処理のみが示されている。ステップ102 ～ステップ104 の処理は，第１実施例（図４）と同じなので，その説明を省略する。

【０１５０】複数のユーザ（クライアント・コンピュータ）のために，複数の（一般的にはユーザの数よりも多くの）ユーザ識別子（発注識別子または取引識別子）と暗号化ユーザ鍵（第１実施例の暗号化鍵に対応）と復号ユーザ鍵（第１実施例の復号鍵に対応）との組があらかじめセキュリティサービス・サーバＣ12で生成される。ユーザ識別子（001～00m）と復号ユーザ鍵46（001～00m）の組，および復号プログラムはセキュリティサービス・サーバＣ12からバーチャルショップ・サーバＳ11に配送される（ステップ121）。

【０１５１】ユーザは入力装置から発注情報（住所，氏名，電話番号，商品番号，クレジット・カード番号等）を入力し，表示画面に表示された注文ボタンをクリックする。

【０１５２】ユーザが注文ボタンをクリックすると，暗号化プログラムの送信要求がクライアント・コンピュータ10からセキュリティサービス・サーバＣ12に送信される（ステップ105 ）。

【０１５３】あるクライアント・コンピュータ10からの送信要求を受信すると，セキュリティサービス・サーバＣ12は，先に生成した複数のユーザ識別子と暗号化ユーザ鍵の組の中から，任意のユーザ識別子と暗号化ユーザ鍵との組を選択し（これらをユーザ識別子（001 ）と暗号化ユーザ鍵（001 ）とする），選び出した暗号化ユーザ鍵（001 ）45を暗号化プログラムに内蔵して，選択したユーザ識別子とともにクライアント・コンピュータ（001 ）10に送信する（ステップ122 ）。

【０１５４】クライアント・コンピュータ（001 ）10は，暗号化ユーザ鍵（001 ）45を内蔵した暗号化プログラムを受信し，実行する。発注情報は，ユーザ識別子を除いて，暗号化ユーザ鍵（001 ）45を用いて暗号化される（ステップ123 ）。

【０１５５】生成された暗号化発注情報と，ユーザ識別

子とが，ネットワーク13を通じてバーチャルショップ・サーバＳ11に送信される（ステップ124 ）。

【０１５６】バーチャルショップ・サーバＳ11は暗号化発注情報と，ユーザ識別子とを受信すると，ユーザ識別子に基づいて，記憶装置にあらかじめ記憶されている複数の復号ユーザ鍵46のなかから，発注情報の暗号化に用いられた暗号化ユーザ鍵45に対応する復号ユーザ鍵（001 ）46を選び出す。この選択した復号ユーザ鍵（001）46を用いて復号プログラムにしたがって暗号化発注情報が復号され，もとの発注情報（平文）が生成される（ステップ125 ）。

【０１５７】暗号化（復号）に用いられる鍵が，ユーザごとにそれぞれ異なるので，特にバーチャルショップ・サーバＳ11における復号処理において，鍵の誤用を防止することができる。

【０１５８】クライアント・コンピュータ10から送信要求を受信するその都度，セキュリティサービス・サーバＣ12は，ユーザ識別子と暗号化ユーザ鍵と復号ユーザ鍵との組を生成してもよい。そして，生成したユーザ識別子と暗号化ユーザ鍵と暗号化プログラムとをクライアント・コンピュータ10に送信し，生成したユーザ識別子と復号ユーザ鍵とをバーチャルショップ・サーバＳ11に送信する。ユーザ識別子はユーザによる商品発注の毎に異なるものが用いられる。この意味でユーザ識別子は発注識別子または取引識別子といってもよい。

【０１５９】ユーザ（クライアント・コンピュータ10）が複数あり，バーチャルショップ・サーバＳ11が複数存在する場合には，図６に示すフローチャートによる処理と，図11に示すフローチャートによる処理とを組み合わせればよい。すなわち，セキュリティサービス・サーバＣ12は，バーチャルショップ・サーバＳ11ごとにユーザ識別子と暗号化ユーザ鍵と復号ユーザ鍵との組を生成し，ユーザ識別子と復号ユーザ鍵の組をショップ識別子とともに各バーチャルショップ・サーバＳ11に配送する。

【０１６０】ショップ識別子は商品情報とともにバーチャルショップ・サーバＳ11からクライアント・コンピュータ10に送信され，その後，クライアント・コンピュータ10からの暗号化プログラムの送信要求とともにセキュリティサービス・サーバＣ12に送信される。

【０１６１】送信要求を受信したセキュリティサービス・サーバＣ12は，ショップ識別子にもとづく複数のユーザ識別子と暗号化ユーザ鍵の組の中から選び出したユーザ識別子と暗号化ユーザ鍵と暗号化プログラムを，クライアント・コンピュータ10に送信する。

【０１６２】第４実施例

図12は第４実施例を示すもので，クライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。第３実施例（図11）と同じ処理についてはその説明を省略する。はじめに，ユーザ識別子と復号ユーザ鍵46との組，通信鍵復号プログラムおよび発注情報復号プログラムがセキュリティサービス・サーバＣ12からバーチャルショップ・サーバＳ11に配送される（ステップ130 ）。

【０１６３】ユーザが注文ボタンをクリックすると，暗号化プログラムの送信要求がクライアント・コンピュータ10からセキュリティサービス・サーバＣ12に送信される（ステップ105 ）。セキュリティサービス・サーバＣ12は，複数のユーザ識別子と暗号化ユーザ鍵の組の中から任意のユーザ識別子（001 ）と暗号化ユーザ鍵（011 ）の組を選び出し，その暗号化ユーザ鍵（001 ）45を内蔵した通信鍵暗号化プログラムと，乱数生成プログラムと，発注情報暗号化プログラムとを，ユーザ識別子（001 ）とともにクライアント・コンピュータ（001 ）10に送信する（ステップ131 ）。

【０１６４】クライアント・コンピュータ10において，はじめに乱数生成プログラムが実行され，通信鍵43が生成される（ステップ112 ）。この通信鍵43を用いて発注情報暗号化プログラムにしたがって発注情報が暗号化される（ステップ113 ）。このとき，ユーザ識別子は暗号化されない。

【０１６５】さらにクライアント・コンピュータ10において，暗号化ユーザ鍵（001 ）45を内蔵した通信鍵暗号化プログラムにしたがって，暗号化ユーザ鍵（001 ）を用いて通信鍵43が暗号化され，暗号化通信鍵44が生成される（ステップ132 ）。暗号化通信鍵44は，ユーザ識別子および暗号化発注情報とともに，バーチャルショップ・サーバＳ11に送信される（ステップ133 ）。

【０１６６】バーチャルショップ・サーバＳ11は，受信したユーザ識別子にもとづいて，記憶装置に記憶されている複数の復号ユーザ鍵46の中から暗号化に用いられた暗号化ユーザ鍵と対応する復号ユーザ鍵（001 ）を選び出す。暗号化通信鍵44は復号ユーザ鍵（001 ）46を用いて通信鍵復号プログラムにしたがって復号され，通信鍵43が得られる（ステップ134 ）。さらに暗号化発注情報は，通信鍵43を用いて発注情報復号プログラムにしたがって復号され，もとの平文の発注情報が得られる（ステップ135 ）。

【０１６７】第５実施例

図13は，第５実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12間のデータ（プログラム）の流れと，クライアント・コンピュータ10における暗号化処理と，サーバＳ11における復号処理の様子を示している。図14は，第５実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。第３実施例（図11）に示すものと同じ処理についてはその説明を省略する。

【０１６８】第５実施例では，公開鍵暗号方式が用いられている。公開鍵暗号方式では，公開鍵51と秘密鍵52の対が用いられる。公開鍵51を用いて暗号化処理が行われ，復号鍵52を用いて復号処理が行われる。

【０１６９】第５実施例において，暗号化処理に用いられる公開鍵と復号処理に用いられる秘密鍵との対は，第３実施例と同様に，ＥＣシステムを利用するユーザの発注処理（ユーザ識別子）ごとに異なる。秘密鍵52とユーザ識別子との組および復号プログラムはバーチャルショップ・サーバＳ11に配送される（ステップ141 ）。

【０１７０】ユーザが入力装置を用いてクライアント・コンピュータ10に発注情報を入力し，注文ボタンをクリックすると，セキュリティサービス・サーバＣ12には暗号化プログラムの送信要求が送信される（ステップ102～ステップ105 ）。

【０１７１】セキュリティサービス・サーバＣ12は，任意のユーザ識別子と公開鍵（これを公開鍵（001 ）51とする）との組および暗号化プログラムをクライアント・コンピュータ（001 ）10に送信する（ステップ142 ）。公開鍵51は他人に知られてもよいので，公開鍵51は単独で送信してもよい。もちろん，公開鍵51を内蔵した暗号化プログラムをクライアント・コンピュータ10に送信してもよい。

【０１７２】暗号化プログラムがクライアント・コンピュータ10によって実行され，発注情報は公開鍵（001 ）51を用いて暗号化される（ステップ143 ）。このとき，ユーザ識別子は暗号化されない。暗号化発注情報は，ユーザ識別子とともにバーチャルショップ・サーバＳ11に送信される（ステップ144 ）。

【０１７３】送信されたユーザ識別子に基づいて，バーチャルショップ・サーバＳ11は，発注情報の暗号化に用いた公開鍵（001 ）51と対をなす秘密鍵52（これを秘密鍵（001 ）52とする）を，あらかじめ配送されている複数の秘密鍵52の中から選び出す。そして，バーチャルショップ・サーバＳ11は復号プログラムを実行する。暗号化発注情報が，暗号化に用いられた公開鍵（001 ）51と対をなす秘密鍵（001）52を用いて復号され，もとの発注情報が得られる（ステップ145 ）。

【０１７４】複数のバーチャルショップ・サーバＳ11が存在する場合には，上述したように，ショップ識別子が用いられる。

【０１７５】第６実施例

図15は，第６実施例におけるクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理と，その流れを示している。第３実施例（図11）と同じ処理についての説明は省略する。

【０１７６】セキュリティサービス・サーバＣ12は公開鍵用暗号化プログラム，秘密鍵用復号プログラム，発注情報暗号化プログラムおよび発注情報復号プログラムを持つ。セキュリティサービス・サーバＣ12は，複数の公開鍵51と秘密鍵52の対をユーザ識別子ごとに生成し，秘密鍵52とユーザ識別子との組，秘密鍵用復号プログラムおよび発注情報復号プログラムをバーチャルショップ・サーバＳ11に配送する（ステップ151 ）。

【０１７７】ユーザが注文ボタンをクリックすると（ステップ105 ），セキュリティサービス・サーバＣ12は暗号化プログラムの送信要求が送信される。セキュリティサービス・サーバＣ12はクライアント・コンピュータ10に，任意の公開鍵51とユーザ識別子（001 とする）との組，公開鍵用暗号化プログラム，発注情報暗号化プログラムを送信する（ステップ152 ）。

【０１７８】はじめに，通信鍵43を用いて発注情報が暗号化される（ステップ153 ）。このとき，ユーザ識別子は暗号化されない。通信鍵43は乱数生成プログラムで生成した乱数であってもよいし（この場合には，最も好ましくはセキュリティサービス・サーバＣ12からクライアント・コンピュータ10に乱数生成プログラムが送信される），ユーザがクライアント・コンピュータ10の入力装置から入力したデータ（ユーザによって任意に決定される数字，記号，アルファベット等の入力の数字列，文字列またはこれらの組合せ）を通信鍵43として用いてもよい。

【０１７９】次に通信鍵43が，公開鍵（001 ）51を用いて公開鍵用暗号化プログラムにしたがって暗号化される（ステップ154 ）。暗号化通信鍵44は，暗号化発注情報およびユーザ識別子とともにバーチャルショップ・サーバＳ11に送信される（ステップ155）。

【０１８０】バーチャルショップ・サーバＳ11は，受信したユーザ識別子にもとづいて，発注情報の暗号化に用いられた公開鍵（001 ）51と対をなす秘密鍵（001 ）52を，あらかじめ配送されている複数の秘密鍵52の中から選び出す。秘密鍵用復号プログラムにしたがって，暗号化通信鍵44が秘密鍵（001 ）52を用いて復号され，通信鍵43が得られる（ステップ156 ）。

【０１８１】つづいて，バーチャルショップ・サーバＳ11は，発注情報復号プログラムを実行する。暗号化発注情報が通信鍵43を用いて復号され，もとの発注情報が得られる（ステップ157 ）。

【０１８２】第７実施例

図16は，第１実施例（図４）に示すクライアント・コンピュータ10，バーチャルショップ・サーバＳ11およびセキュリティサービス・サーバＣ12のそれぞれが行う処理に，さらにプログラムと鍵の消去処理を加えた処理の流れを示している。第１実施例（図４）と同じ処理の説明は省略する。

【０１８３】ユーザが注文ボタンをクリックすると（ステップ105 ），クライアント・コンピュータ10にはセキュリティサービス・サーバＣ12から，暗号化鍵41を内蔵した暗号化プログラムとともに，それらを消去する消去

プログラムが送信される（ステップ161 ）。暗号化鍵41を内蔵した暗号化プログラムおよび消去プログラムは，ともにクライアント・コンピュータ10の記憶装置に記憶される。

【０１８４】暗号化プログラムにしたがって暗号化鍵41を用いて発注情報が暗号化される（ステップ107 ）。暗号化発注情報はその後，ネットワーク13を介してバーチャルショップ・サーバＳ11に送信される（ステップ108 ）。

【０１８５】暗号化発注情報の送信を終えたクライアント・コンピュータ10は，記憶装置から消去プログラムを読み出し，これを実行する（ステップ162 ）。消去プログラムは暗号化発注情報がバーチャルショップ・サーバＳ11に送信された直後に実行されるようにプログラミングされている。消去プログラムにより，暗号化プログラムと暗号化鍵41（暗号化鍵を内蔵した暗号化プログラム）はコンピュータ10の内部メモリから消去される。

【０１８６】暗号化プログラムと暗号化鍵とを消去することによって，第三者が暗号化プログラムまたは暗号化鍵を入手することが困難となるので，第三者の解読行為を未然に防止することができ，ＥＣシステムにおける暗号化処理および復号処理の安全性を高めることができる。ユーザについて言えば，送信される暗号化プログラムおよび暗号化鍵を，ＥＣシステムにおける１回限りの利用のみに制限することができる。暗号化に用いた暗号化プログラムおよび暗号化鍵が暗号化発注情報の送信後は存在しなくなるので，ユーザがこれらを悪用（たとえば，ＥＣシステムの利用以外に用いること）を防止することができる。

【０１８７】図16に示す消去プログラムによる暗号化プログラムおよび暗号化鍵の消去手段は，第１実施例（図４）に基づいているが，他の実施例においても，暗号化プログラム，乱数生成プログラム等のプログラムと，鍵データとを消去できることはいうまでもない。また，暗号化（復号）アルゴリズムとして周知のものを用いる場合には，暗号化鍵やユーザ鍵などの鍵データのみを消去するようにしてもよい。逆に，鍵データの消去を行わずに，暗号化プログラム，乱数生成プログラムなどのプログラムのみを消去してもよい。任意のプログラムのみまたは鍵データのみ（たとえば暗号化プログラムのみ）を消去するようにすることもできる。同様にして，バーチャルショップ・サーバＳ11に配送されたプログラムおよび鍵データを消去してもよい。

【図面の簡単な説明】

【図１】第１実施例におけるＥＣ（エレクトロニック・コマース）システムの全体的構成を示す。

【図２】(A) は暗号アルゴリズムの一例を，(B)はＳボックスの一例を示す。

【図３】第１実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバおよびセキュリティサービス・サーバ間のプログラムを含むデータの流れと，暗号化処理および復号処理を示す。

【図４】第１実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図５】第１実施例の変形例におけるクライアント・コンピュータ，バーチャルショップ・サーバおよびセキュリティサービス・サーバ間のプログラムを含むデータの流れと，暗号化処理および復号処理を示す。

【図６】第１実施例の変形例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図７】第２実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバおよびセキュリティサービス・サーバ間のプログラムを含むデータの流れと，暗号化処理および復号処理を示す。

【図８】第２実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図９】第３実施例におけるＥＣ（エレクトロニック・コマース）システムの全体的構成を示す。

【図１０】第３実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバおよびセキュリティサービス・サーバ間のプログラムを含むデータの流れと，暗号化処理および復号処理を示す。

【図１１】第３実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図１２】第４実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図１３】第５実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバ間のプログラムを含むデータの流れと，暗号化処理および復号処理を示す。

【図１４】第５実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

【図１５】第６実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサービス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

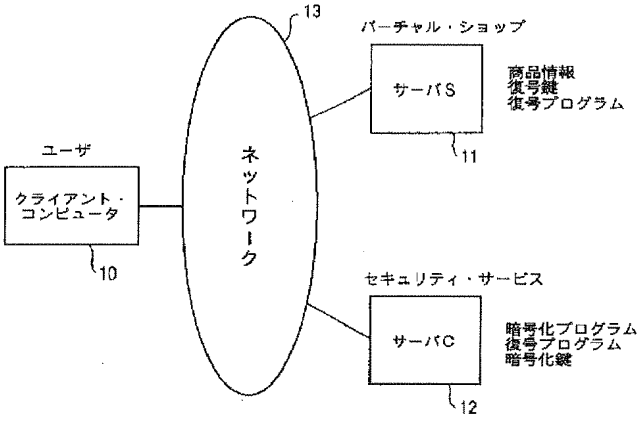
【図１６】第７実施例におけるクライアント・コンピュータ，バーチャルショップ・サーバ，セキュリティサー

ビス・サーバにおいてそれぞれ行われる処理の流れを示すフローチャートである。

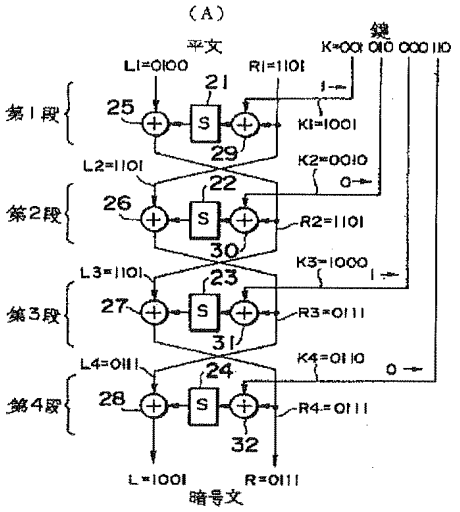
【符号の説明】

10　クライアント・コンピュータ
11　バーチャルショップ・サーバ
12　セキュリティサービス・サーバ
13　ネットワーク
41　暗号化鍵
＊42　復号鍵
43　通信鍵
44　暗号化通信鍵
45　暗号化ユーザ鍵
46　復号ユーザ鍵
51　公開鍵
52　秘密鍵

【図１】



【図２】

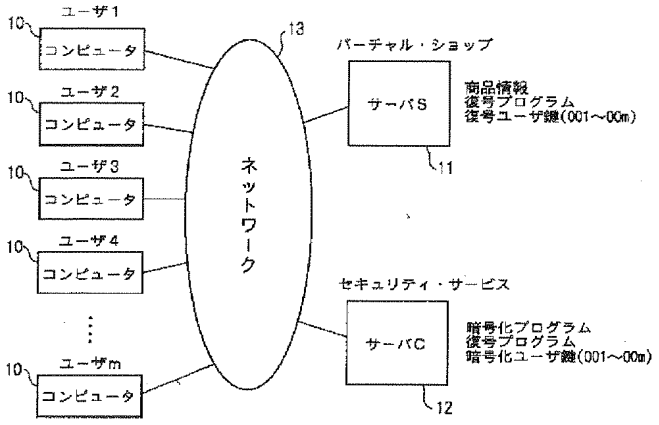


(B)

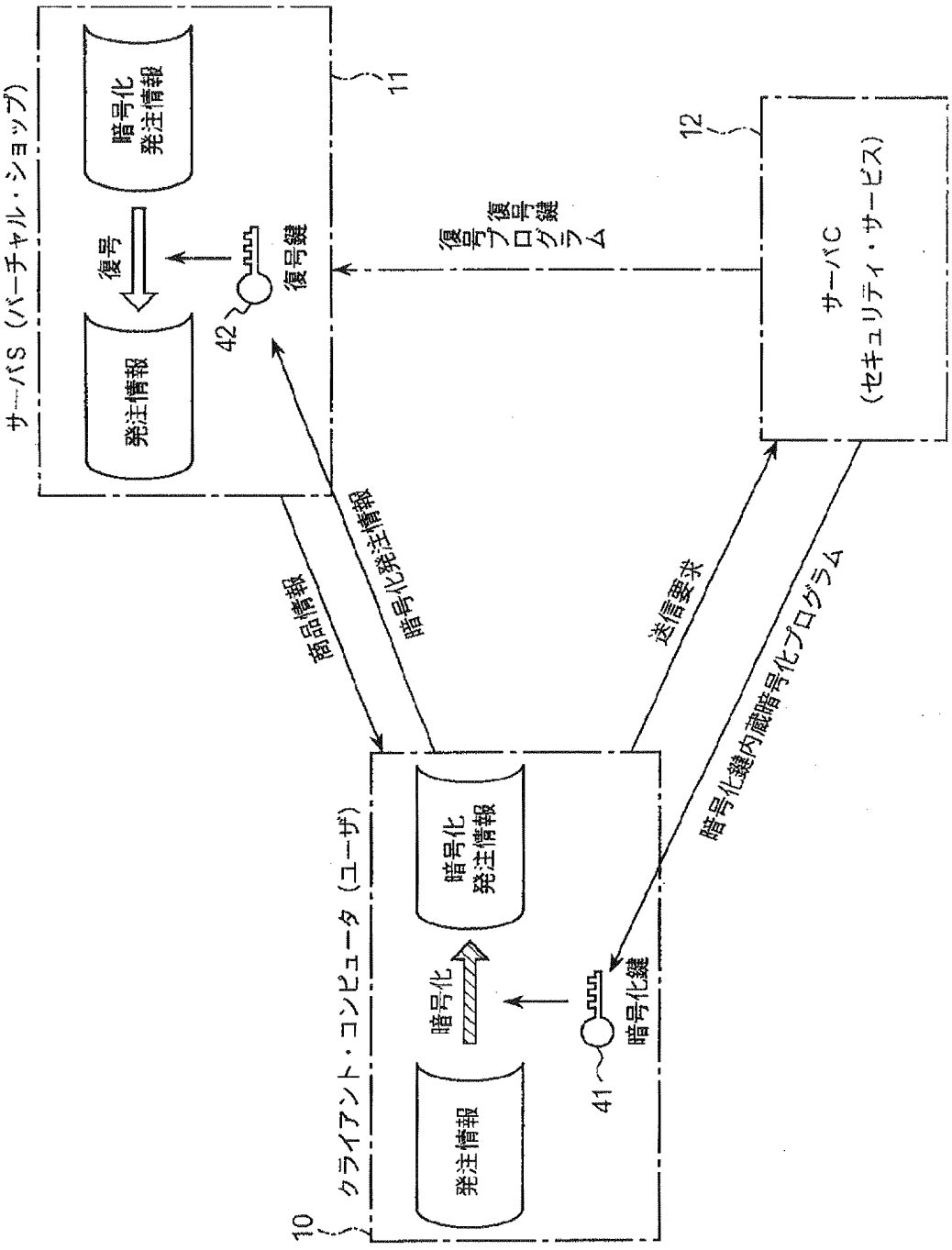
入力	出力
0	7
1	14
2	15
3	13
4	9
5	0
6	1
7	2
8	4
9	8
10	3
11	6
12	12
13	11
14	5
15	10

Sボックス

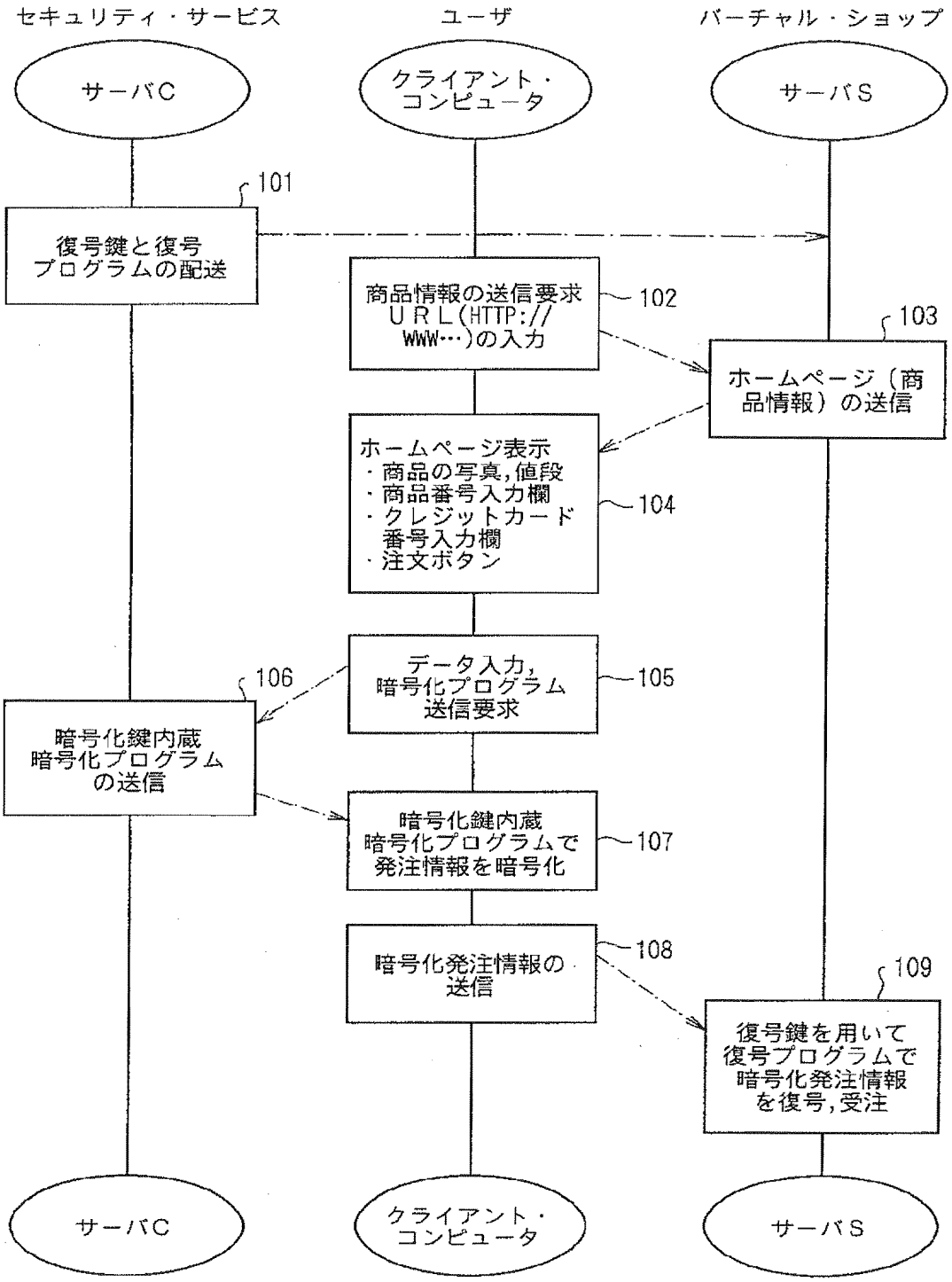
【図９】



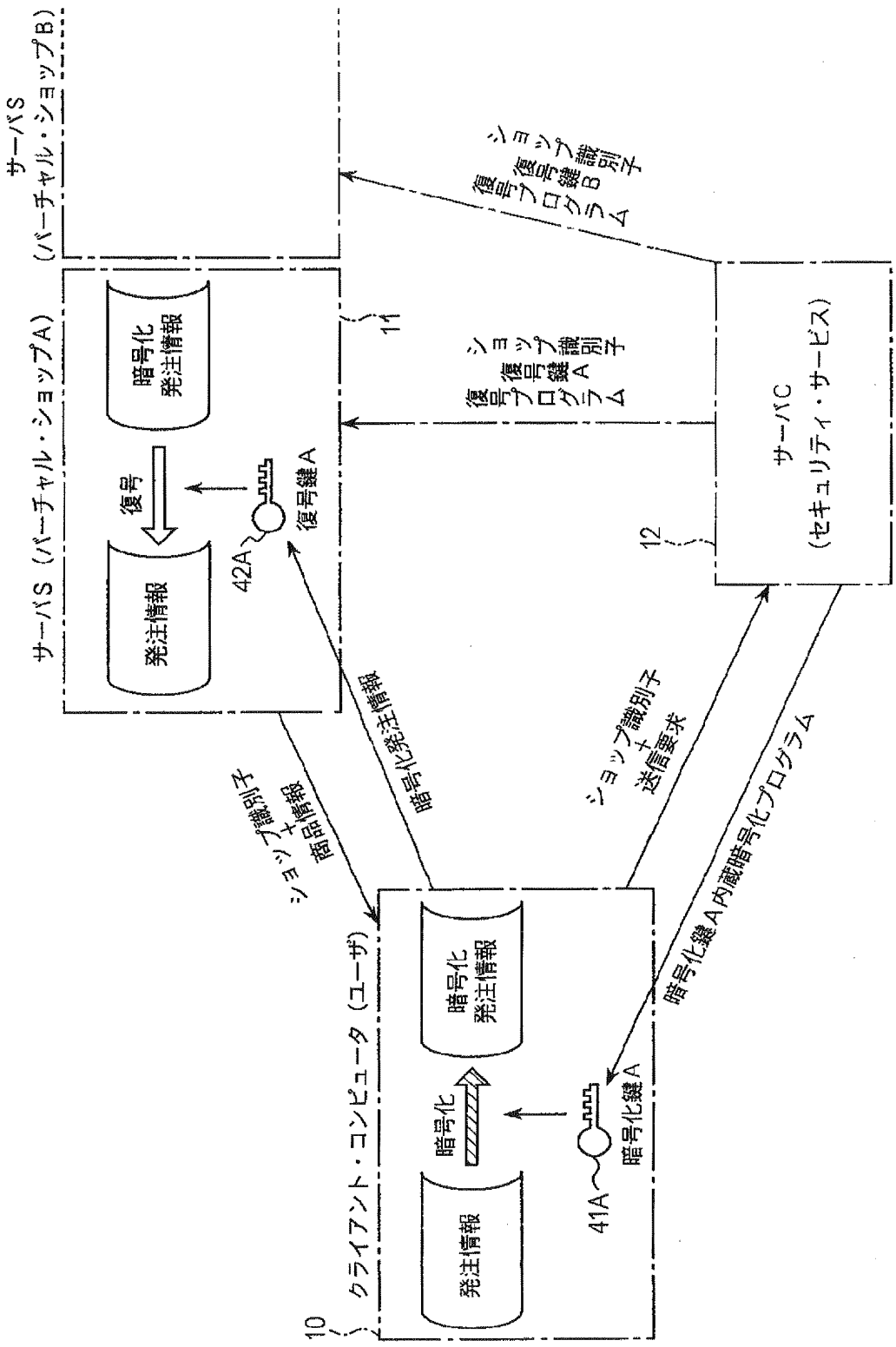
【図３】


サーバS（バーチャル・ショップ）
暗号化
発注情報
復号
発注情報
42
復号鍵
11
12
復号プログラム
サーバC
（セキュリティ・サービス）
商品情報
暗号化発注情報
送信要求
暗号化鍵内蔵暗号化プログラム
暗号化
発注情報
暗号化鍵
41
クライアント・コンピュータ（ユーザ）
10

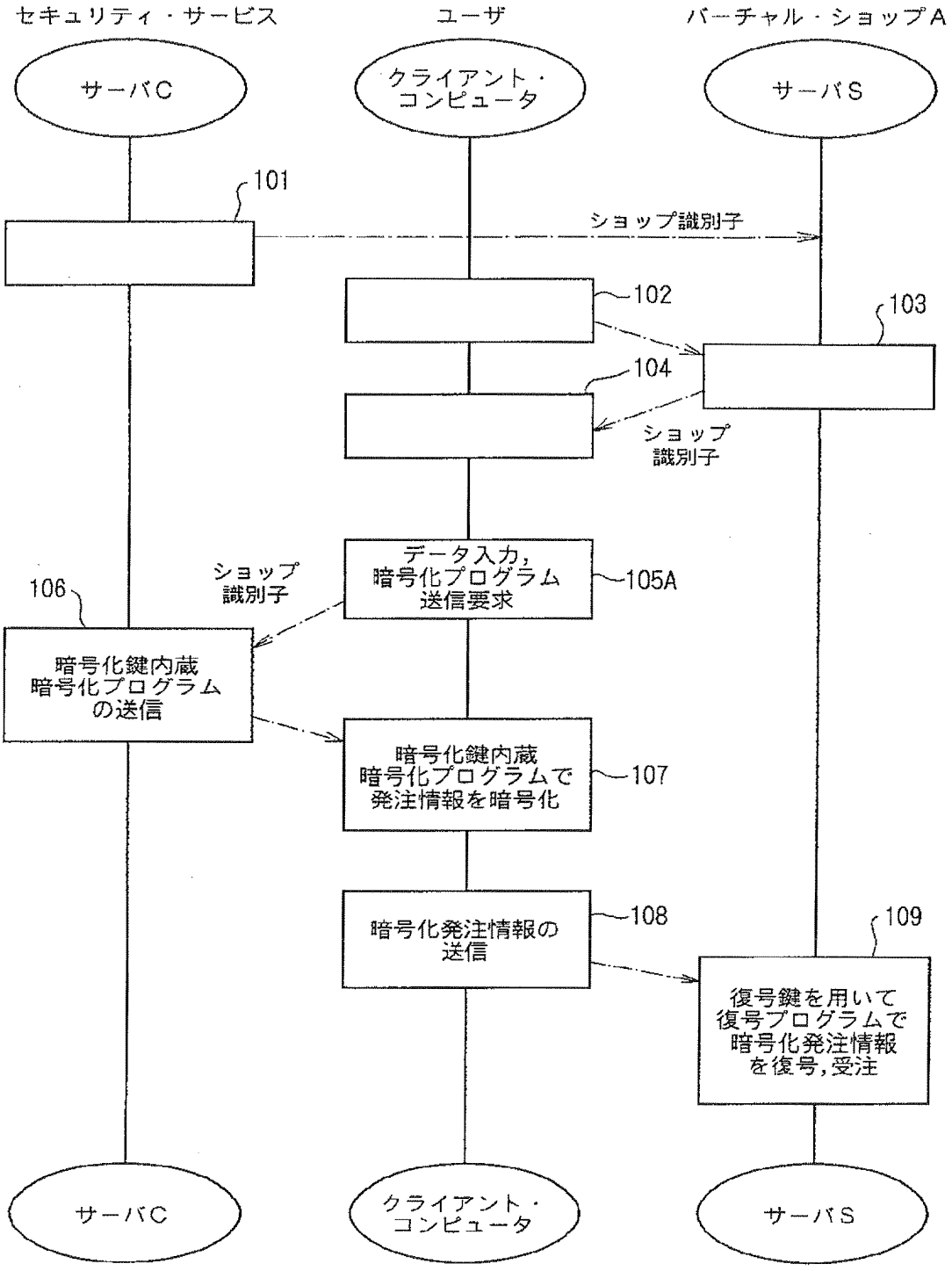
【図４】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ
サーバS
101
復号鍵と復号プログラムの配送
商品情報の送信要求 URL(HTTP://WWW…)の入力
102
103
ホームページ（商品情報）の送信
ホームページ表示
・商品の写真,値段
・商品番号入力欄
・クレジットカード番号入力欄
・注文ボタン
104
データ入力,暗号化プログラム送信要求
105
106
暗号化鍵内蔵暗号化プログラムの送信
暗号化鍵内蔵暗号化プログラムで発注情報を暗号化
107
暗号化発注情報の送信
108
109
復号鍵を用いて復号プログラムで暗号化発注情報を復号,受注
サーバC
クライアント・コンピュータ
サーバS

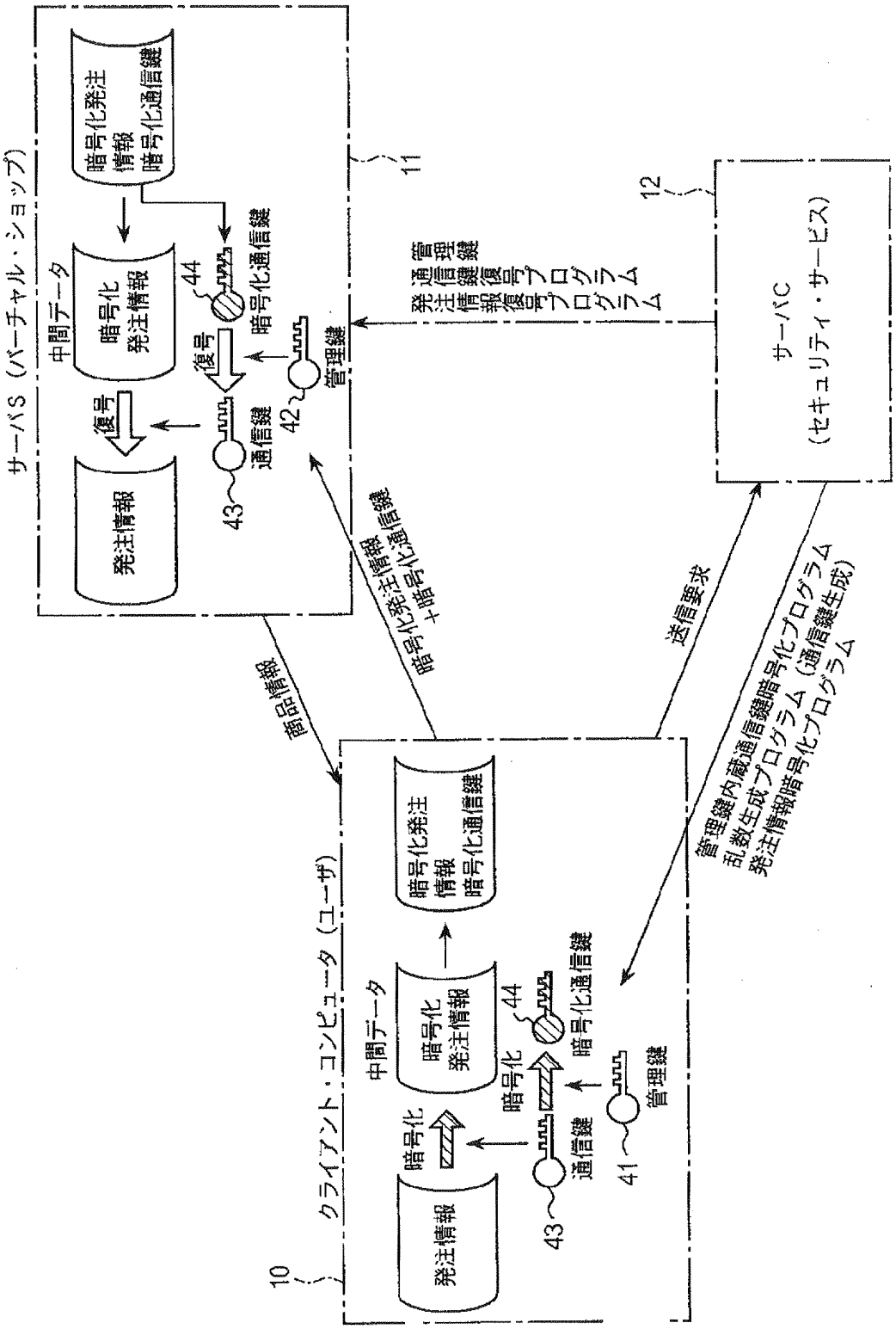
【図５】


サーバS
（バーチャル・ショップB）
サーバS（バーチャル・ショップA）
暗号化
発注情報
復号
発注情報
42A
復号鍵A
11
ショップ識別子
復号プログラム
ショップ識別子
復号鍵Bプログラム
サーバC
（セキュリティ・サービス）
12
ショップ識別子
＋
商品情報
暗号化発注情報
ショップ識別子
＋
送信要求
暗号化鍵A内蔵暗号化プログラム
クライアント・コンピュータ（ユーザ）
暗号化
発注情報
暗号化
発注情報
41A
暗号化鍵A
10

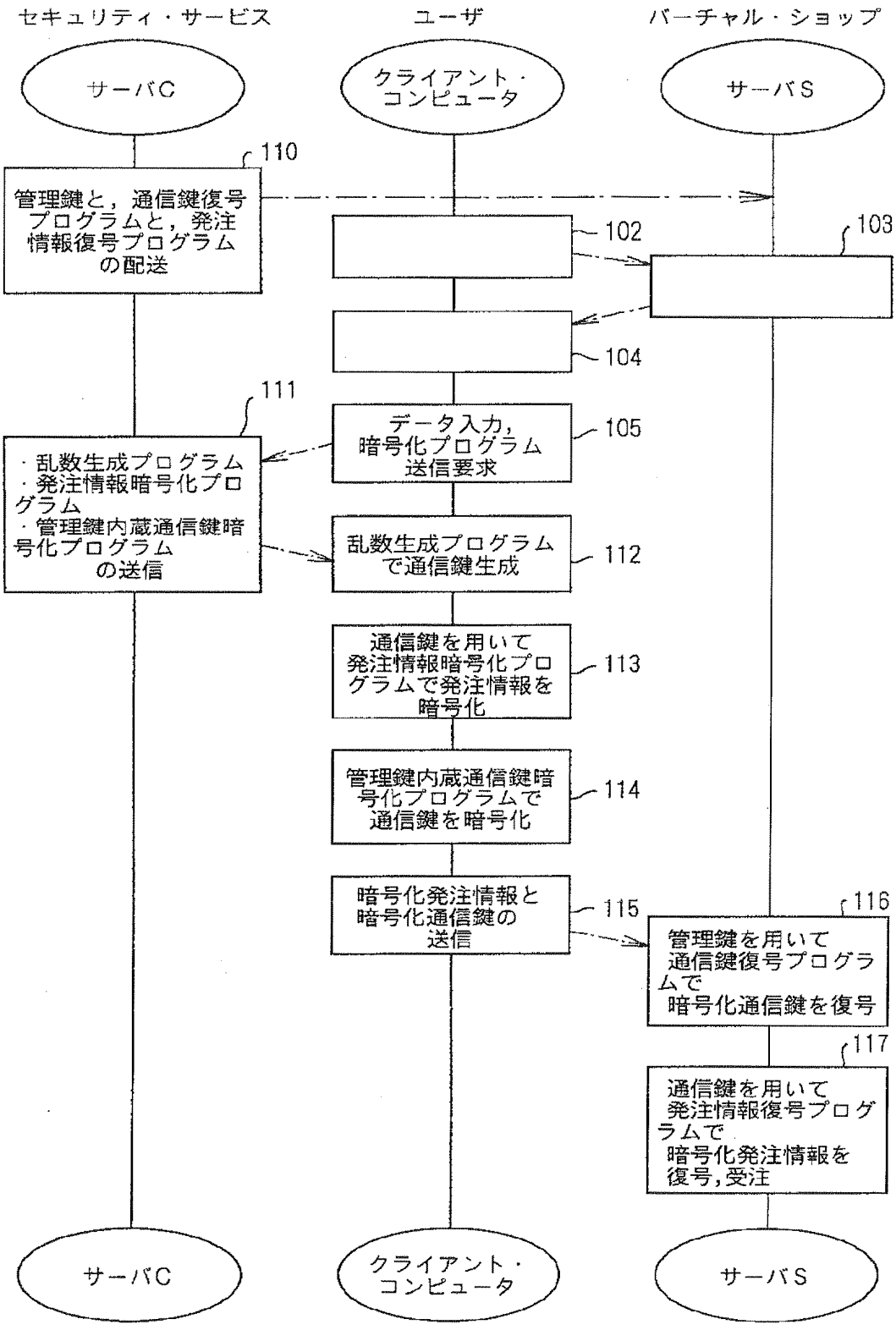
【図６】


セキュリティ・サービス
ユーザ
バーチャル・ショップA
サーバC
クライアント・コンピュータ
サーバS
101
ショップ識別子
102
103
104
ショップ識別子
データ入力，暗号化プログラム送信要求
105A
106
ショップ識別子
暗号化鍵内蔵暗号化プログラムの送信
暗号化鍵内蔵暗号化プログラムで発注情報を暗号化
107
暗号化発注情報の送信
108
109
復号鍵を用いて復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ
サーバS

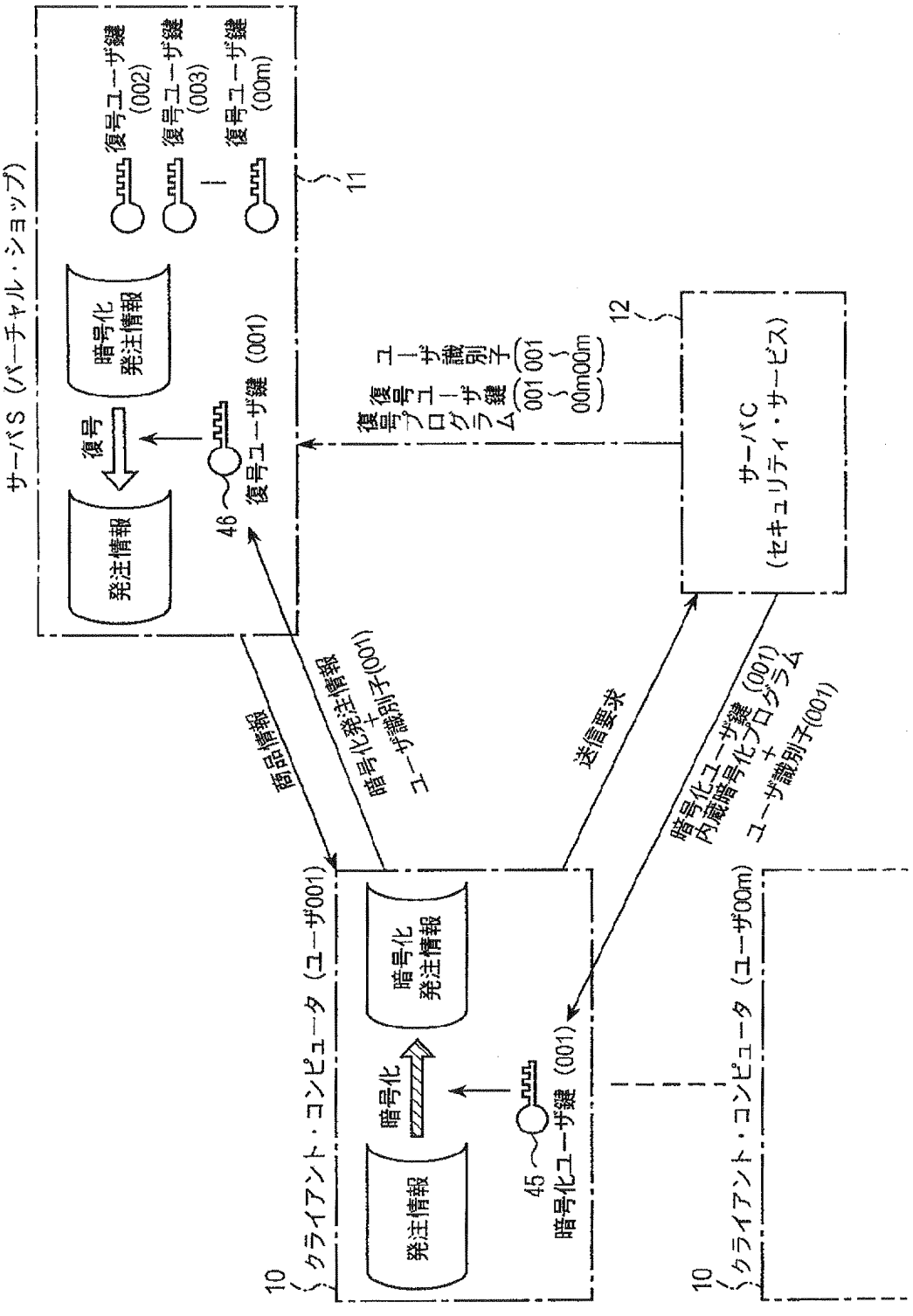
【図７】


サーバS（バーチャル・ショップ）
暗号化発注情報 暗号化通信鍵
中間データ
暗号化発注情報
44
暗号化通信鍵
復号
復号
発注情報
43
通信鍵
42
管理鍵
11
12
管理鍵 発注情報復号プログラム 通信鍵復号プログラム
サーバC（セキュリティ・サービス）
商品情報
暗号化発注情報＋暗号化通信鍵
送信要求
管理鍵内蔵通信鍵暗号化プログラム 乱数生成プログラム 発注情報暗号化プログラム（通信鍵生成）
暗号化発注情報 暗号化通信鍵
中間データ
暗号化発注情報
44
暗号化
暗号化通信鍵
暗号化
通信鍵
管理鍵
41
43
発注情報
10
クライアント・コンピュータ（ユーザ）

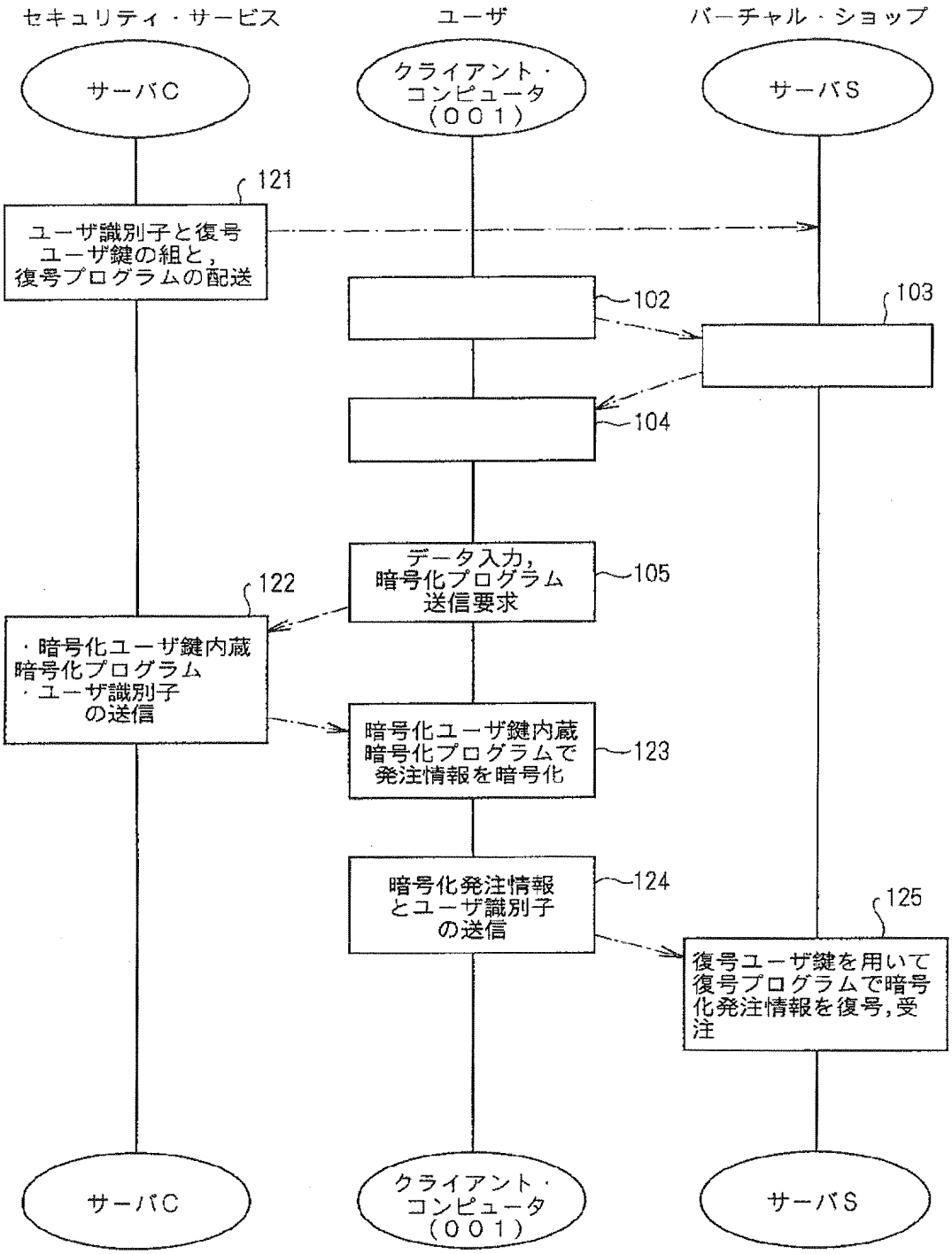
【図８】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ
サーバS
110
管理鍵と，通信鍵復号プログラムと，発注情報復号プログラムの配送
102
103
104
111
データ入力，暗号化プログラム送信要求
105
・乱数生成プログラム
・発注情報暗号化プログラム
・管理鍵内蔵通信鍵暗号化プログラム
の送信
乱数生成プログラムで通信鍵生成
112
通信鍵を用いて発注情報暗号化プログラムで発注情報を暗号化
113
管理鍵内蔵通信鍵暗号化プログラムで通信鍵を暗号化
114
暗号化発注情報と暗号化通信鍵の送信
115
116
管理鍵を用いて通信鍵復号プログラムで暗号化通信鍵を復号
117
通信鍵を用いて発注情報復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ
サーバS

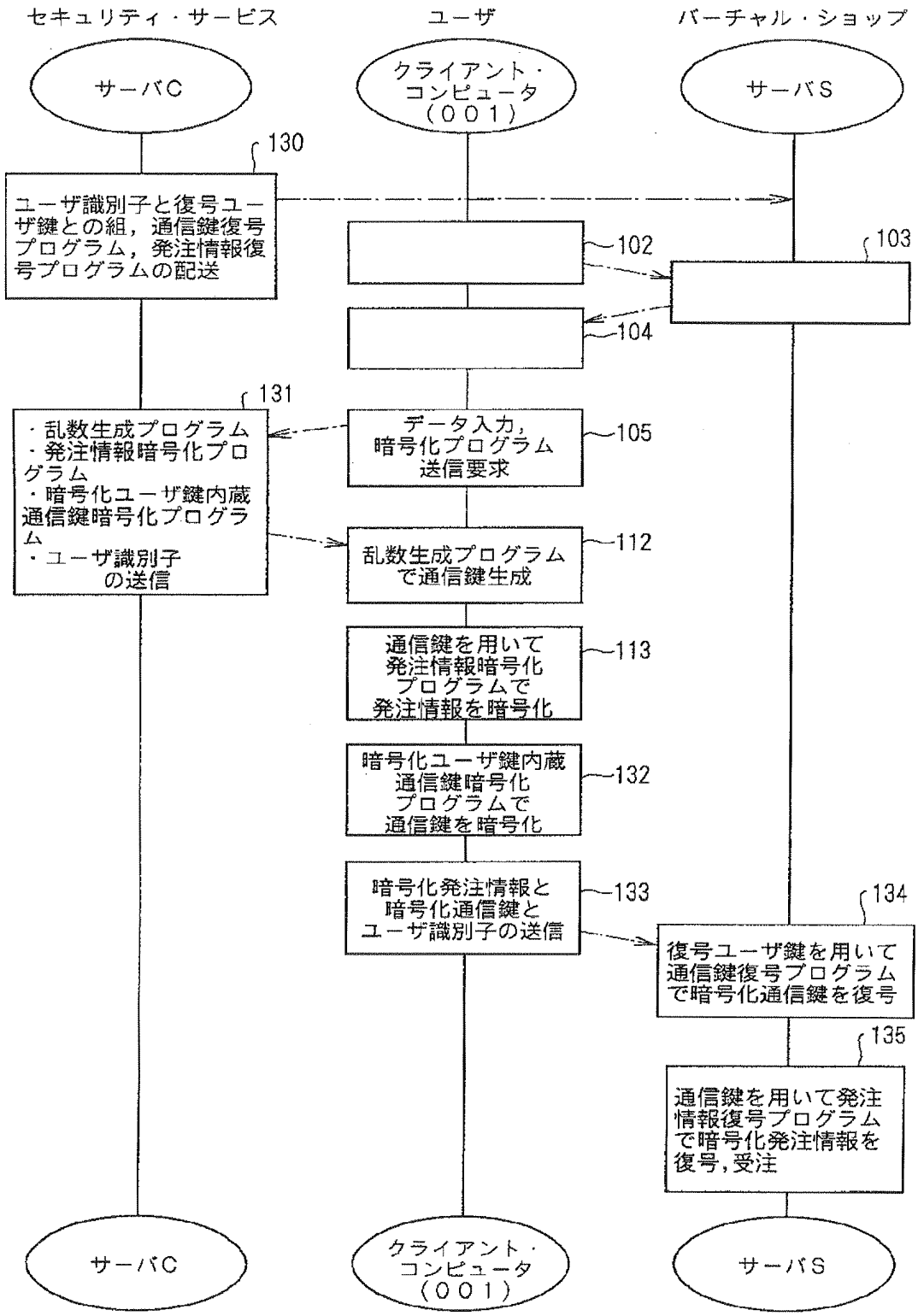
【図１０】


サーバＳ（バーチャル・ショップ）
復号ユーザ鍵 (002)
復号ユーザ鍵 (003)
復号ユーザ鍵 (00m)
11
暗号化 発注情報
復号
発注情報
46
復号ユーザ鍵（001）
復号プログラム
ユーザ識別子 (001 ～ 00m)
12
サーバＣ (セキュリティ・サービス)
商品情報
暗号化発注情報 ＋ ユーザ識別子(001)
送信要求
暗号化ユーザ鍵 (001) 内蔵暗号化プログラム ＋ ユーザ識別子(001)
10
クライアント・コンピュータ（ユーザ001）
暗号化 発注情報
暗号化
発注情報
45
暗号化ユーザ鍵（001）
10
クライアント・コンピュータ（ユーザ00m）

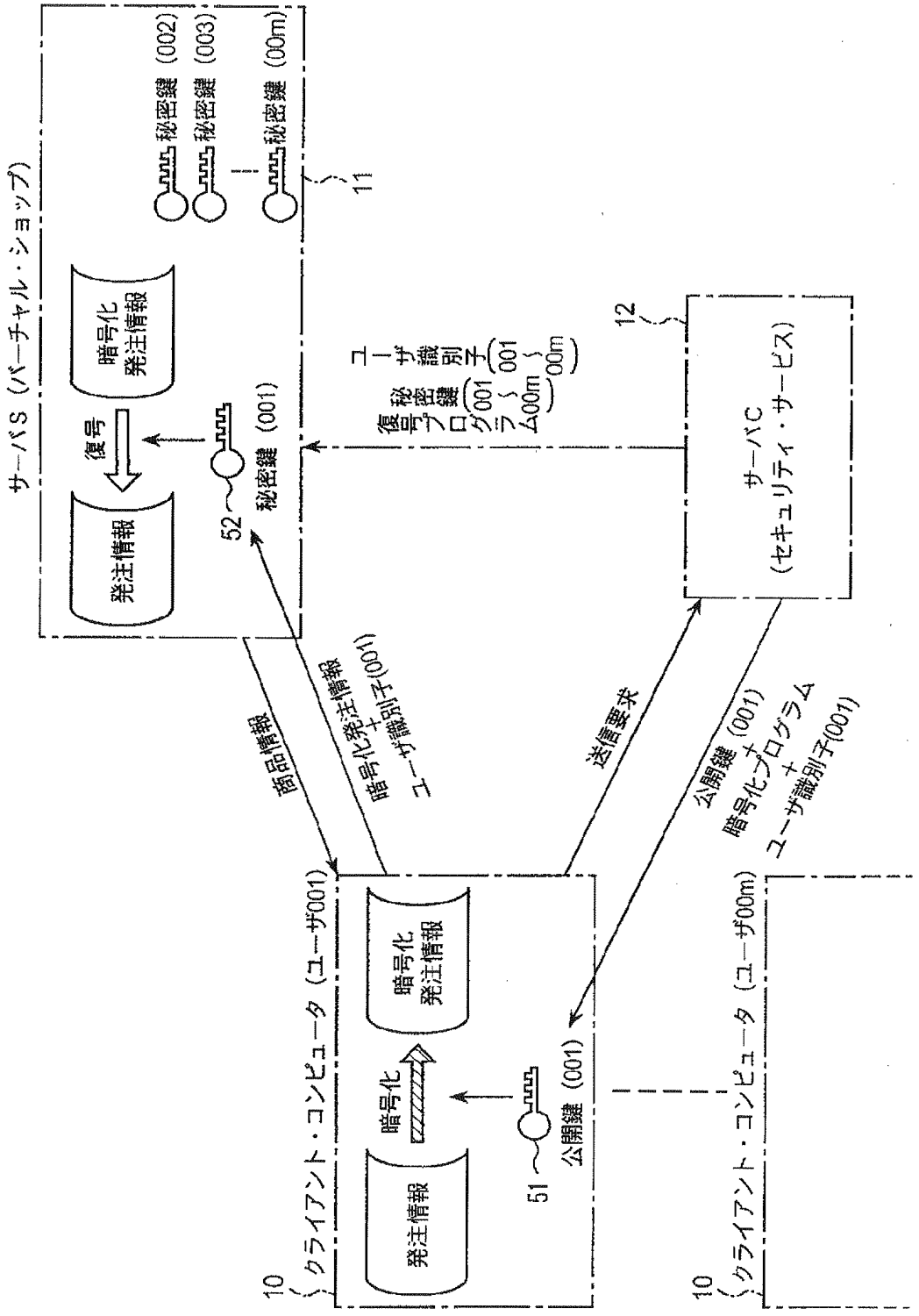
【図１１】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ（００１）
サーバS
121
ユーザ識別子と復号ユーザ鍵の組と，復号プログラムの配送
102
103
104
データ入力，暗号化プログラム送信要求
105
122
・暗号化ユーザ鍵内蔵暗号化プログラム
・ユーザ識別子の送信
暗号化ユーザ鍵内蔵暗号化プログラムで発注情報を暗号化
123
暗号化発注情報とユーザ識別子の送信
124
125
復号ユーザ鍵を用いて復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ（００１）
サーバS

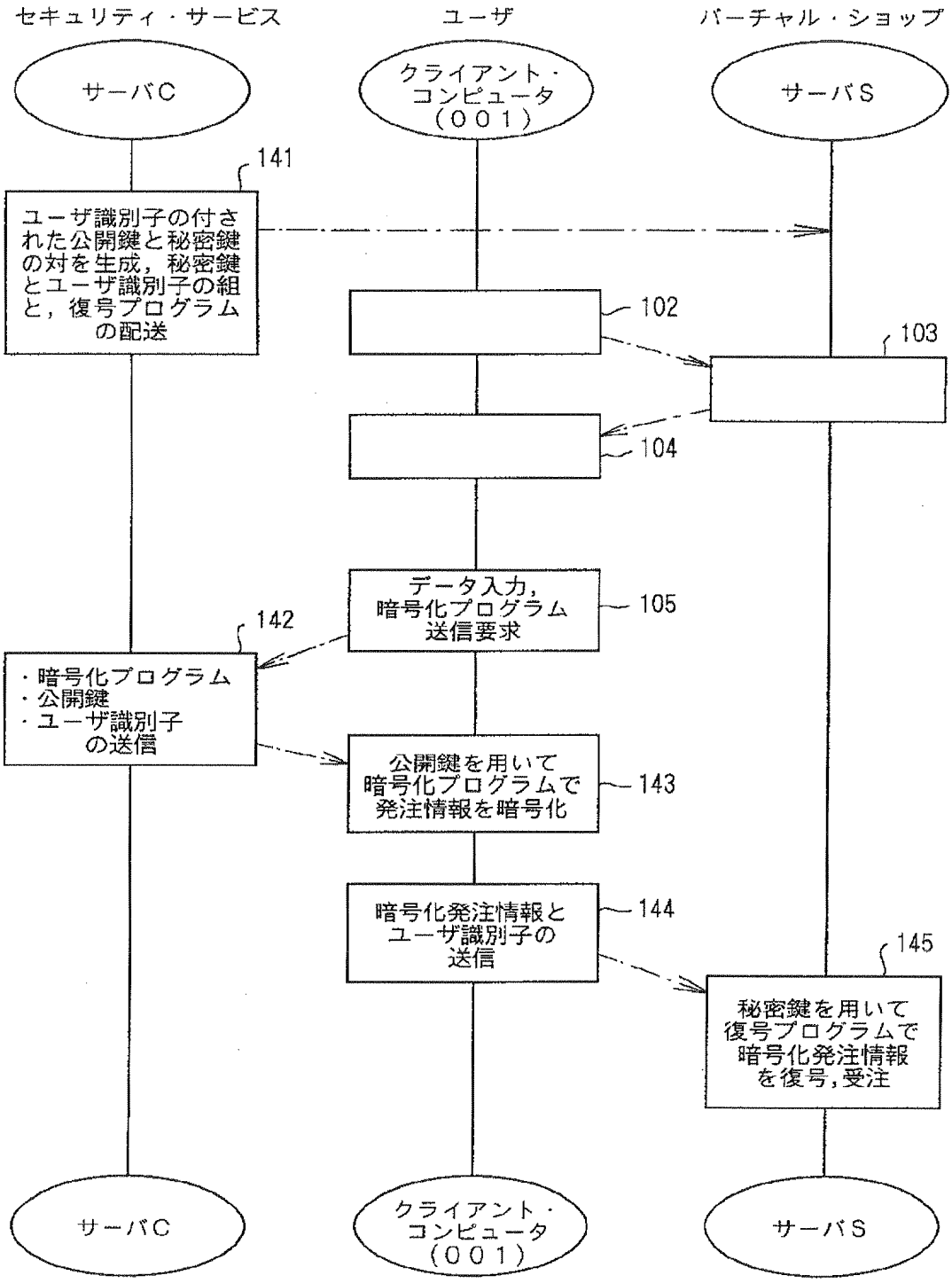
【図１２】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ（００１）
サーバS
130
ユーザ識別子と復号ユーザ鍵との組，通信鍵復号プログラム，発注情報復号プログラムの配送
102
103
104
131
・乱数生成プログラム
・発注情報暗号化プログラム
・暗号化ユーザ鍵内蔵通信鍵暗号化プログラム
・ユーザ識別子の送信
データ入力，暗号化プログラム送信要求
105
乱数生成プログラムで通信鍵生成
112
通信鍵を用いて発注情報暗号化プログラムで発注情報を暗号化
113
暗号化ユーザ鍵内蔵通信鍵暗号化プログラムで通信鍵を暗号化
132
暗号化発注情報と暗号化通信鍵とユーザ識別子の送信
133
134
復号ユーザ鍵を用いて通信鍵復号プログラムで暗号化通信鍵を復号
135
通信鍵を用いて発注情報復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ（００１）
サーバS

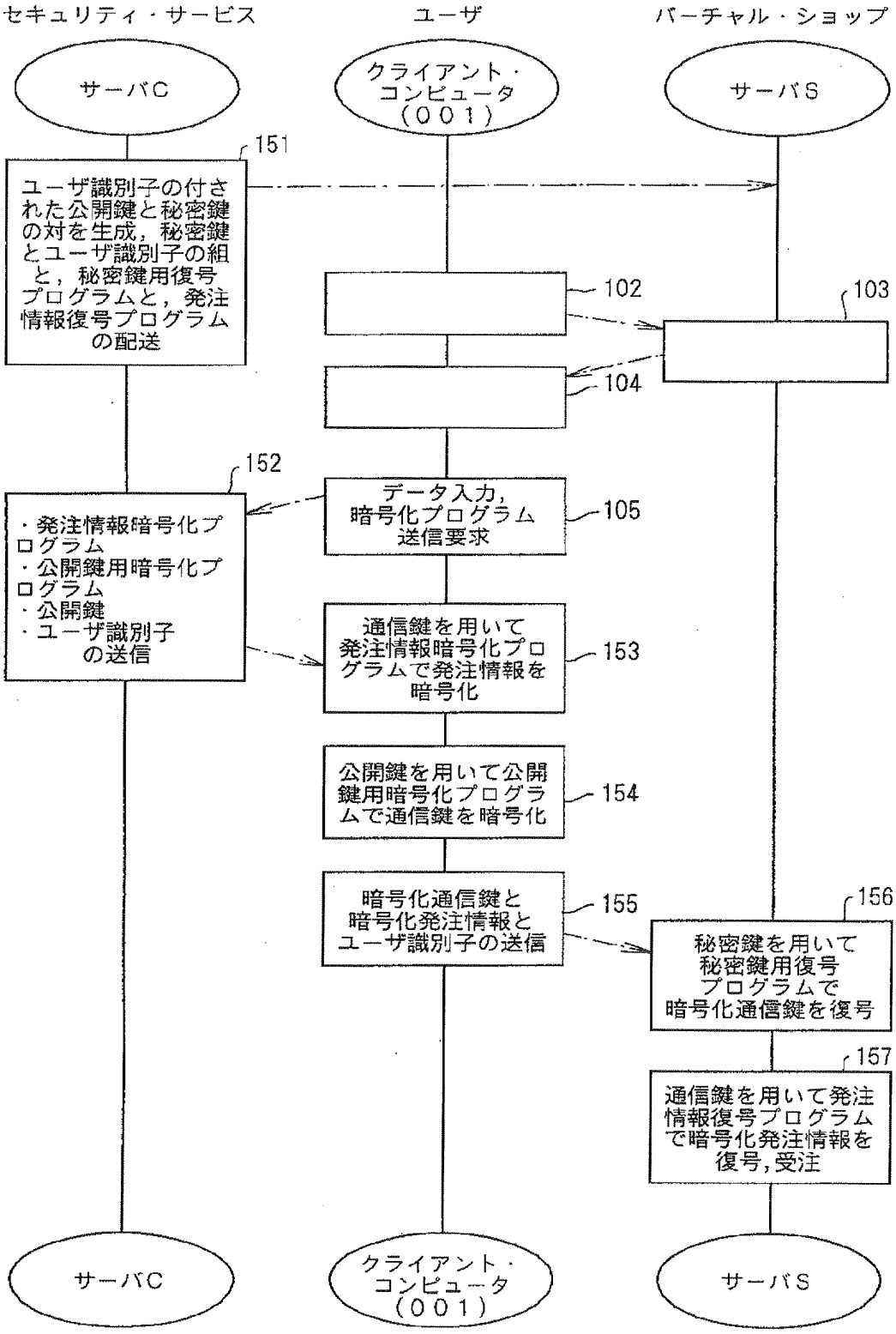
【図１３】


サーバS（バーチャル・ショップ）
秘密鍵（002）
秘密鍵（003）
秘密鍵（00m）
11
暗号化発注情報
復号
発注情報
52
秘密鍵（001）
ユーザ識別子（001～00m）
復号プログラム
12
サーバC
（セキュリティ・サービス）
商品情報
暗号化発注情報＋ユーザ識別子（001）
送信要求
公開鍵（001）
暗号化プログラム＋ユーザ識別子（001）
暗号化発注情報
暗号化
発注情報
51
公開鍵（001）
10
クライアント・コンピュータ（ユーザ001）
10
クライアント・コンピュータ（ユーザ00m）

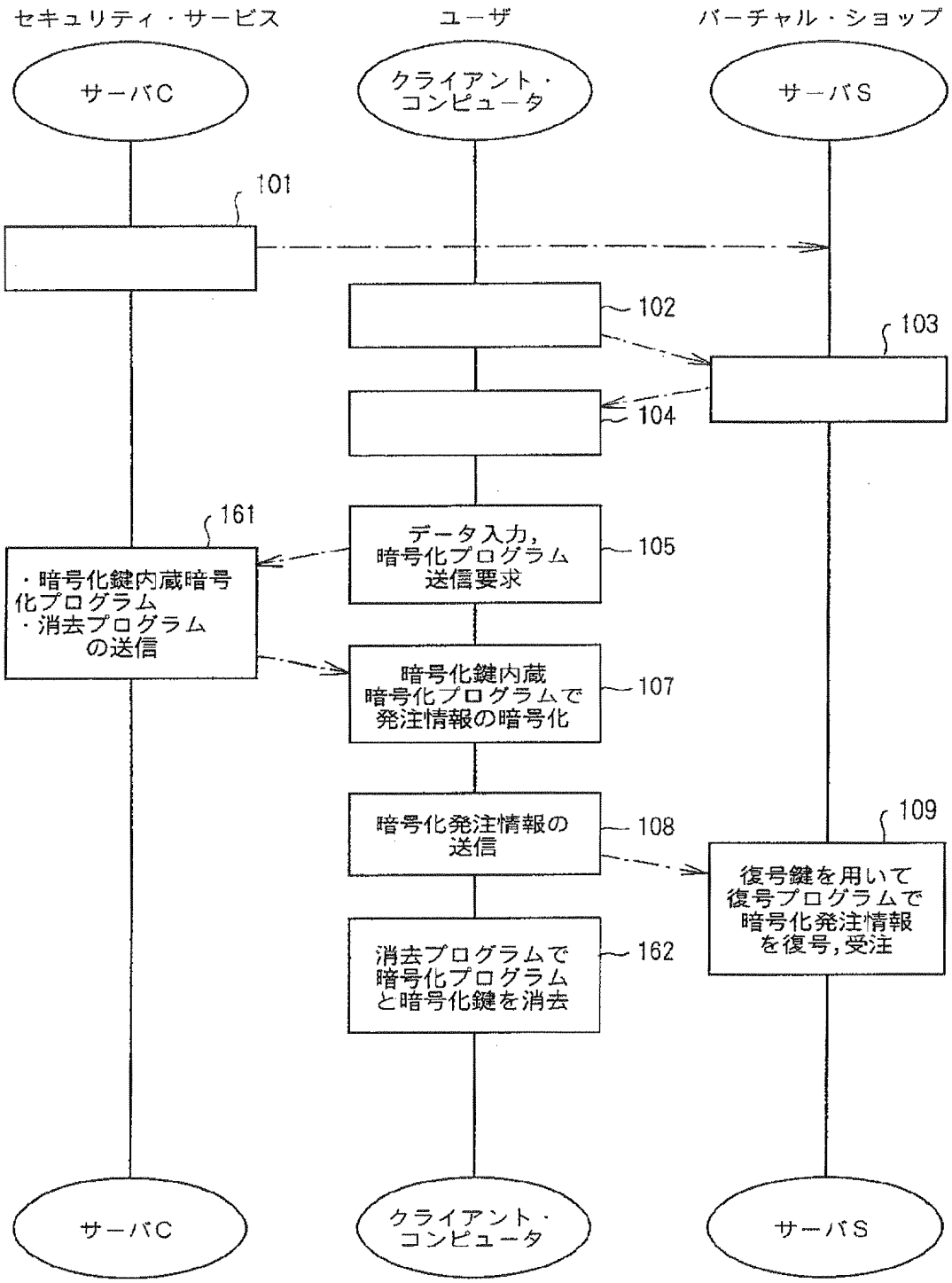
【図１４】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ（００１）
サーバS
141
ユーザ識別子の付された公開鍵と秘密鍵の対を生成，秘密鍵とユーザ識別子の組と，復号プログラムの配送
102
103
104
データ入力，暗号化プログラム送信要求
105
142
・暗号化プログラム
・公開鍵
・ユーザ識別子
の送信
公開鍵を用いて暗号化プログラムで発注情報を暗号化
143
暗号化発注情報とユーザ識別子の送信
144
145
秘密鍵を用いて復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ（００１）
サーバS

【図１５】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ（００１）
サーバS
151
ユーザ識別子の付された公開鍵と秘密鍵の対を生成，秘密鍵とユーザ識別子の組と，秘密鍵用復号プログラムと，発注情報復号プログラムの配送
102
103
104
152
データ入力，暗号化プログラム送信要求
105
・発注情報暗号化プログラム
・公開鍵用暗号化プログラム
・公開鍵
・ユーザ識別子
の送信
通信鍵を用いて発注情報暗号化プログラムで発注情報を暗号化
153
公開鍵を用いて公開鍵用暗号化プログラムで通信鍵を暗号化
154
暗号化通信鍵と暗号化発注情報とユーザ識別子の送信
155
156
秘密鍵を用いて秘密鍵用復号プログラムで暗号化通信鍵を復号
157
通信鍵を用いて発注情報復号プログラムで暗号化発注情報を復号，受注
サーバC
クライアント・コンピュータ（００１）
サーバS

【図１６】


セキュリティ・サービス
ユーザ
バーチャル・ショップ
サーバC
クライアント・コンピュータ
サーバS
101
102
103
104
161
データ入力，暗号化プログラム送信要求
105
・暗号化鍵内蔵暗号化プログラム
・消去プログラム
の送信
暗号化鍵内蔵暗号化プログラムで発注情報の暗号化
107
暗号化発注情報の送信
108
109
復号鍵を用いて復号プログラムで暗号化発注情報を復号，受注
消去プログラムで暗号化プログラムと暗号化鍵を消去
162
サーバC
クライアント・コンピュータ
サーバS